Vägverket

Publikation 2004:178

Kommunikationsprotokoll inom ITS

– en inventering av kommunikationsprotokoll inom intelligenta transportsystem och tjänster

Examensarbete av Daniel Ekström

Department of Science and Technology
Linköpings Universitet
SE-601 74 Norrköping, Sweden

Institutionen för teknik och naturvetenskap
Linköpings Universitet
601 74 Norrköping

Dokumentkontroll

DOKUMENTDATUM: 2004-12-01

PROJEKTINFORMATION
Examensarbete Kommunikationsprotokoll inom ITS
/Daniel Ekström
Handledare Vägverket: Johnny Alf Stri
VV Diarienr:

DOKUMENTINFORMATION
Dokumenttitel: Kommunikationsprotokoll inom ITS - en inventering av kommunikationsprotokoll inom intelligenta transportsystem och tjänster
Dokumentstatus: Offentlig

FÖRFATTARE
Huvudförfattare: Daniel Ekström
Övriga medförfattare:

DOKUMENTDISTRIBUTION
Kontaktperson Johnny Alf 0243-75696

Referat

Vägverkets uppgift är att utveckla och upprätthålla en långsiktig hållbar och samhällsekonomisk effektiv transportförsörjning för medborgare och näringsliv. Inom området ITS används i dagsläget en mängd olika kommunikationsprotokoll och internationellt finns ett antal kommunikationsstandarder tillgängliga. Kunskapen om dessa är begränsad och hittills har Vägverket ej ställt några direkta krav på kommunikationsprotokoll vid upphandlingar av systemlösningar utan accepterat vad leverantören erbjudit. Detta är något som Vägverket vill ändra på, samtidigt som trenden går mot öppna kommunikationsprotokoll bland tillverkare och leverantörer.

Aktuella kommunikationsprotokoll och internationella kommunikationsstandarder har inventeras och beskrivits. De väsentligaste problemen med användandet av en mängd olika kommunikationsprotokoll är avsaknaden av interoperabilitet och utbytbarhet av apparater. Enda relevanta lösningen för att upphäva dessa problem är en standardisering av kommunikationen.

Fördelarna med en standardisering är många, medan nackdelarna främst är ekonomiska. För att utröna en standardiserings långsiktiga ekonomiska påverkan samt för att få fram ett kostnads/nyttoförhållande är en ekonomisk analys önskvärd. Rekommendationen är att en standardisering genomförs om kostnaderna anses rimliga och resurserna finns tillgängliga.

Examensarbete
LITH-ITN-KTS-EX--04/021--SE

Kommunikationsprotokoll inom ITS

Daniel Ekström

2004-06-04

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

LITH-ITN-KTS-EX--04/021--SE

Kommunikationsprotokoll inom ITS

Examensarbete utfört i kommunikations- och transportsystem vid Linköpings Tekniska Högskola, Campus Norrköping

Daniel Ekström

Handledare: Johnny Alf, Vägverket
Handledare: Clas Rydergren, LiU
Examinator: Di Yuan, LiU

Norrköping 2004-06-04

Avdelning, Institution
Division, Department

Institutionen för teknik och naturvetenskap

Department of Science and Technology

Datum
Date

2004-06-04

Språk
Language

■ Svenska/Swedish
☐ Engelska/English

☐ _____

Rapporttyp
Report category

Examensarbete

☐ B-uppsats
☐ C-uppsats
■ D-uppsats

☐ _____

ISBN

_____

_____

ISRN LITH-ITN-KTS-EX--04/021--SE

Serietitel och serienummer
Title of series, numbering

ISSN

_____

URL för elektronisk version

http://www.ep.liu.se/exjobb/itn/2004/kts/021

Titel **Kommuikationsprotokoll inom ITS**
Title Communication protocols within ITS

Författare **Daniel Ekström**
Author

Sammanfattning
Abstract

Vägverkets uppgift är att utveckla och upprätthålla en långsiktig hållbar och samhällsekonomisk effektiv transportförsörjning för medborgare och näringsliv. Inom området ITS-används i dagsläget en mängd olika kommunikationsprotokoll och internationellt finns ett antal kommunikationsstandarder tillgängliga. Kunskapen om dessa är begränsad och hittills har Vägverket ej ställt några direkta krav på kommunikationsprotokoll vid upphandlingar av systemlösningar utan accepterat vad leverantören erbjudit. Detta är något som Vägverket vill ändra på, samtidigt som trenden går mot öppna kommunikationsprotokoll bland tillverkare och leverantörer.

Aktuella kommunikationsprotokoll och internationella kommunikationsstandarder har inventeras och beskrivits. De väsentligaste problemen med användandet av en mängd olika kommunikationsprotokoll är avsaknaden av interoperabilitet och utbytbarhet av apparater. Enda relevanta lösningen för att upphäva dessa problem är en standardisering av kommunikationen.

Fördelarna med en standardisering är många, medan nackdelarna främst är ekonomiska. För att utröna en standardiserings långsiktiga ekonomiska påverkan samt för att få fram ett kostnads/nyttoförhållande är en ekonomisk analys önskvärd. Rekommendationen är att en standardisering genomförs om kostnaderna anses rimliga och resurserna finns tillgängliga. Främst då fördelarna med utbytbarhet av apparater, interoperabilitet och bättre konkurrensvillkor är stora samt att de enda relevanta nackdelarna är av ekonomisk art.

Vid en standardisering bör den befintliga standard användas som bäst uppfyller rekommendationer gällande tekniska aspekter och vilka ITS-områden som omfattas. Rekommendationer har även tagits fram för vilka länder som bör omfattas av en standardisering. Lämpligt är att de nordiska länderna omfattas då dessa har liknande synsätt och normer. För att klargöra vilken av de befintliga standarderna som är bäst lämpad att använda vid en standardisering har en utvärdering av standarderna har genomförts. Denna utvärdering har klargjort att den standard som bäst följer rekommendationerna är den amerikanska standarden NTCIP.

Viktigt att ha i åtanke är att NTCIP inte kan implementeras som det är, utan att ändringsarbete krävs för att anpassa den till svenska/nordiska normer och synsätt. Oavsett vad som beslutas angående en standardisering så är det viktigt att det sker inom en förhållandevis snar framtid och att det meddelas berörda aktörer.

Nyckelord **Kommunikationsprotokoll, Kommunikationsstandarder, Intelligenta Transport System, ITS, Protokoll, Standard, Standardisera, Vägverket**

Keyword Communication protocols, Communications Standards, Intelligent Transport Systems, ITS, Protocol, Standard, Standardization, Swedish National Road Administration

Förord

Användandet av olika kommunikationsprotokoll inom Intelligenta Transport System (ITS) medför vissa problem. Examensarbetet syftar till att inventera vilka kommunikationsprotokoll respektive kommunikationsstandarder som finns tillgängliga inom ITS-området, jämföra dessa och ta fram rekommendationer för hur Vägverket ska agera.

Examensarbetet är utfört på avdelningen ITS-sektionen, Vägverket. Till grund för rapporten ligger litteraturstudier, samtal och intervjuer med personer med god branschkännedom.

Resultatet av arbetet är denna rapport. Den beskriver bland annat den problembild som finns med användandet av olika kommunikationsprotokoll, aktuella kommunikationsprotokoll och kommunikationsstandarder, vad som bör göras och hur det bör göras för att problemen som finns med användandet av olika protokoll ska upphävas.

Examinator har Di Yuan, Institutionen för Teknik och Naturvetenskap (ITN), Linköpings Universitet varit och som handledare har jag haft Johnny Alf, Vägverket och Clas Rydergren, ITN, Linköpings Universitet.

Borlänge 2004-05-26

Daniel Ekström

Sammanfattning

Vägverkets uppgift är att utveckla och upprätthålla en långsiktig hållbar och samhällsekonomisk effektiv transportförsörjning för medborgare och näringsliv. Inom området ITS används i dagsläget en mängd olika kommunikationsprotokoll och internationellt finns ett antal kommunikationsstandarder tillgängliga. Kunskapen om dessa är begränsad och hittills har Vägverket ej ställt några direkta krav på kommunikationsprotokoll vid upphandlingar av systemlösningar utan accepterat vad leverantören erbjudit. Detta är något som Vägverket vill ändra på, samtidigt som trenden går mot öppna kommunikationsprotokoll bland tillverkare och leverantörer.

Aktuella kommunikationsprotokoll och internationella kommunikationsstandarder har inventeras och beskrivits. De väsentligaste problemen med användandet av en mängd olika kommunikationsprotokoll är avsaknaden av interoperabilitet och utbytbarhet av apparater. Enda relevanta lösningen för att upphäva dessa problem är en standardisering av kommunikationen.

Fördelarna med en standardisering är många, medan nackdelarna främst är ekonomiska. För att utröna en standardiserings långsiktiga ekonomiska påverkan samt för att få fram ett kostnads/nyttoförhållande är en ekonomisk analys önskvärd. Rekommendationen är att en standardisering genomförs om kostnaderna anses rimliga och resurserna finns tillgängliga. Främst då fördelarna med utbytbarhet av apparater, interoperabilitet och bättre konkurrensvillkor är stora samt att de enda relevanta nackdelarna är av ekonomisk art.

Vid en standardisering bör den befintliga standard användas som bäst uppfyller rekommendationer gällande tekniska aspekter och vilka ITS-områden som omfattas. Rekommendationer har även tagits fram för vilka länder som bör omfattas av en standardisering. Lämpligt är att de nordiska länderna omfattas då dessa har liknande synsätt och normer. För att klargöra vilken av de befintliga standarderna som är bäst lämpad att använda vid en standardisering har en utvärdering av standarderna har genomförts. Denna utvärdering har klargjort att den standard som bäst följer rekommendationerna är den amerikanska standarden NTCIP.

Viktigt att ha i åtanke är att NTCIP inte kan implementeras som det är, utan att ändringsarbete krävs för att anpassa den till svenska/nordiska normer och synsätt. Oavsett vad som beslutas angående en standardisering så är det viktigt att det sker inom en förhållandevis snar framtid och att det meddelas berörda aktörer.

Summary

The Swedish National Road Administrations task is to develop and maintain a long-term lasting and community economic effective transport support for citizens and industry. Within the ITS sphere are many different communication protocols used today and internationally there are a number of communication standards available. The knowledge about those is limited and so far hasn't the Swedish National Road Administration set any absolute requirements on the communication protocols at purchase of system solutions but accepted what the supplier offered. This is something that the Swedish Road Administration wants to change; at the same time is the trend moving against open communication protocols among suppliers.

It has been made an inventory of existing communication protocols and international communications standards and all have been described. The essential problems with the use of many different communication protocols are the loss of interoperability and interchange ability. Only relevant solution to abolish these problems is to standardize the communication.

The benefits of standardization are many, while the disadvantages mainly are economical. Too find out a standardizations long-term economical influence and too get a cost/benefit ratio is an economical analyse desirable. The recommendation is that standardization is carried out if the costs are considered reasonable and resources are available, mainly because the benefits interchange ability, interoperability and competition conditions are great and that the only relevant disadvantages are of economical art.

At standardization should the existing standard be used, that best full fills the recommendations about technical aspects and which ITS-areas who are covered. A recommendation has also been done for which countries that should be covered by standardization. Suitable are that the Nordic countries are covered, because they have a similar approach and norms. To elucidate which of the existing standards who are best suited to use at standardization has an evaluate of the standards been done. This evaluate elucidated that the standard who best follow the recommendations are the American standard NTCIP.

Important to have in mind is that NTCIP can't be implemented as it are; a change work has to be done to adjust it to Swedish/Nordic approach and norms. Regardless of what is decided about standardization is it important that it is done in relatively soon future and that touched participants get informed.

Innehållsförteckning

1 Inledning

I dagsläget används en mängd olika kommunikationsprotokoll (hädanefter kallat protokoll) inom ITS-området, det finns även ett antal internationella kommunikationsstandarder (hädanefter kallat standarder) som är tänkbara att använda för samma ändamål. Vägverket har begränsade kunskaper om dessa och har hittills inte ställt några direkta krav på dem vid upphandlingar.

Användande av olika protokoll skapar problem, främst med att apparater som stödjer olika typer av protokoll inte kan kommunicera med varandra och att de i de flesta fall inte kan använda sig av samma kommunikationsnätverk. Att apparater stödjer samma protokoll betyder inte automatiskt att de kan kommunicera med varandra, för att kunna kommunicera med varandra måste de även kunna förstå varandras meddelanden, vilket kräver att meddelandenas datainnehåll till stor del måste vara beskrivet på samma sätt.

Dessa problem är önskvärda att upphäva, vilket är fullt möjligt. Denna rapport försöker ge svar på hur detta kan ske och granskar de för- och nackdelar en lösning ger. Rekommendationer har tagits fram för vad en lösning bör uppfylla och standarder har utvärderas för att se vilka/vilken som uppfyller rekommendationerna bäst.

2 Bakgrund och syfte

Vägverkets uppgift är att utveckla och upprätthålla en långsiktig hållbar och samhällsekonomisk effektiv transportförsörjning för medborgare och näringsliv. Detta kan definieras i sex delmål som Vägverket ska inrikta sitt arbete mot. Dessa är: ett tillgängligt transportsystem, ett jämställt transportsystem, en positiv regional utveckling, en hög transportkvalitet, en god miljö samt en säker miljö.

Ett hjälpmedel för att nå dessa mål är att utnyttja IT inom trafiken och här finns en otrolig stor potential att effektivisera vägtrafiken. Med trafikinformatik eller ITS (Intelligenta Transport System) menas att man tillämpar IT-lösningar inom vägtransportsystemet. Det finns ett vitt spektra av olika tillämpningar inom ITS-området. Exempel på sådana är trafikinformation via variabla skyltar, avancerad trafiksignalstyrning, ISA (Intelligent stöd för anpassning av hastighet) och trafikinformation till mobila enheter.

I dagsläget finns en rad kommunikationsprotokoll och kommunikationsstandarder som används i tillämpningar inom ITS-området. Exempel på dessa är NTCIP, TLS och en rad andra som används vid omställbara vägmärken, trafiksignaler etc. Kunskapen om dessa är begränsad och hittills har Vägverket ej ställt några direkta krav på kommunikationsprotokoll vid upphandlingar av systemlösningar utan accepterat det som leverantören erbjudit. Detta är något som Vägverket vill ändra på, samtidigt som trenden går mot öppna protokoll bland tillverkare och leverantörer.

Syftet med arbetet är att göra en inventering av de kommunikationsprotokoll och kommunikationsstandarder som finns tillgängliga inom ITS-området, jämföra dessa och ta fram rekommendationer för hur Vägverket ska agera.

3 Omfattning och övergripande mål

För att ett protokoll skall tas med i denna rapport skall det användas inom ITS. Protokoll som ej används idag och är inaktuella p.g.a. föråldrad teknik eller liknande omfattas ej av rapporten. I de fall när kommunikationsstandarder består av en protokollstack, beskrivs ej de standardprotokoll som ingår i protokollstacken. En protokollstack är en samling av protokoll.

Arbetet ska resultera i en omfattande rapport om funktioner och möjligheter med varje protokoll. Protokollen ska jämföras på en hög teknisk nivå. Rekommendationer ska tas fram för hur Vägverket kan hantera de problem som finns på grund av den mängd olika protokoll som används i dagsläget. Rapporten ska vara skriven på ett sådant sätt att den ska vara läsbar för läsare som har begränsade kunskaper inom ämnet.

4 Uttryck och förkortningar

Nedan introduceras förkortningar och uttryck som används i rapporten. Lämpligtvis används denna lista för att slå upp förkortningar och uttryck som är okända för läsaren. Önskas mer information eller förklaring av uttryck hänvisas till facklitteratur.

ACK	Acknowledgement
ADU	Application Data Unit, ramen i Modbus
AS-Interface	Buss med enkel installationsteknik där både strömförsörjning och data överförs
ASN.1	Abstract Syntax Notation – 1 är ett formellt språk för beskrivning av information som ska bearbetas av en dator
ASCII	American Standard Code for Information Interchange, definierar bit innehållet hos seriellt överförda meddelanden
ASTIN	ASsociation of TRaffic Industries in the Netherlands
AASHTO	American Association of State Highway and Transportation Officials
ATIS	Advanced Traveller Information System
ATM	Asynchronous Transfer Mode
ATM/SONET	Asynchronous Transfer Mode / Synchronous Optical Network
BER	Basic Encoding Rules är en serie av procedurer för beskrivning av överföringssyntax för typer som definieras av ASN.1 Överföringssyntax är den verkliga representationen av oktetter som från en nätverksenhet till en annan. Måste användas tillsammans med SNMP.
Broadcast	Ett meddelande skickas till flera mottagere
BTPPL	Basis Transport Paket Protokoll Layer, OCIT: s egenutvecklade Outstations protokoll
C2C	Förkortning för central-till-central (Center-to-Center)
C2F	Förkortning för central-till-fält (Center-to-Field)
CAN	Controller Area Network, CAN är ett seriellt bussystem speciellt anpassat för att koppla ihop intelligenta apparater för att skapa intelligenta system eller subsystem

CanOpen	Standardiserat applikationsskiktsprotokoll optimerat för inneslutna nätverk (främst Controller Area Network, CAN)
CiA	CAN in Automation, organisation som står bakom CAN och CanOpen.
COM/DCOM	Component Object Model, Distributed COM
CORBA	Common Object Request Broker Architecture Protocol
CRC	Cyclic Redundancy Check, säkerställer informationsinnehållet i ett meddelande
DATEX	DATa EXchange Protocol
DE	Data-Endgeräte-Kanal (data-slutapparat-kanal), en av två logiska adresseringsnivåer i TLS.
DP	Decentral Periferi, Protokoll i Profibus
DPM#	DP master klass # (1 eller 2)
EIA/TIA-232	se RS232
EIA/TIA-485	se RS485
Ethernet	Är det vanligast förekommande protokollet i lager 1 och 2 i OSI modellen, för kommunikation på LAN.
FDDI	Fiber Distributed Data Interface
FG	Funktionsgruppe (funktionsgrupp), en av två logiska adresseringsnivåer i TLS.
FHWA	Federal Highway Administration
Fletchers algorithm	Enkel provsummealgoritm
FTP	File Transfer Protocol
Frame	se Header
Gateway	Förmedlar kontakt mellan två nätverk med olika mjukvara och hårdvara
HDLC	High-Level Data Link Control
Header	Meddelanderam som används för att lägga till bland annat adresser och felkontroll

HMI	Human Machine Interface
I/O	Input/Output
I/O-koncentrator	Aggregerar och utvärderar data från de anslutna I/O-portarna samt överlämnar parametrar och ställkommandon till de anslutna I/O-portarna.
IEC	International Electrotechnical Commission, ett internationellt (huvudsakligen europeiskt) organ för standardisering
IETF	Internet Engineering Task Force
IM	Incident Management
Instations	Gränssnittsområde i OCIT för kommunikation mellan centraler och komponenter
Interoperabilitet	Förmågan att en mångfald av apparater, oftast av olika typ, problemfritt kan verka tillsammans i ett system med gemensamt ändamål, exempelvis använda samma kommunikationskanal.
IP	Internet Protocol
IPI	Initial Protocol Identifier
IRT	Isochronous Real Time
ISO	International Organization for Standardization
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation System
IVER	Initiatiefgroep VErkeersregeltechnici Rijkswaterstaat en Provincies (Initiative Group of Traffic Control Engineers of Department of Public Works and Provinces)
IVERA	Namnet är en kombination av IVER och ASTIN som är två av de bakomliggande organisationerna
LAN	Local Area Network är ett nät som används för lokal kommunikation inom ett begränsat område.
LRC	Longitudinal Redundancy Checking, säkerställer informationsinnehållet i ett meddelande
Master/slav protokoll	Ett master/slav system har en nod (master noden) som utfärdar kommandon till en av slav noderna och bearbetar svar. Slav noden

	överför normalt inte data utan en fråga från master noden och kommunicerar inte med andra noder.
MBP	Manchester Coding (M) och Bus Powering (BP), överföringsteknik i skikt 1 i OSI-modellen.
MIB	Management Information Base
Modbus	Industristandard för kommunikation
NACK	Not acknowledgement
NEMA	National Electronics Manufacturers Association
NRZ	Non Return to Zero, kodningstyp för bit representation
NTCIP	National Transportation Communications for ITS Protocol
NULL	se T2
OCA	Open Traffic Systems City Association e.V
OCIT	Open Communication Interface for Road Traffic Control Systems
ODG	OCIT Developer Group
OER	Octet Encoding Rules
OSI modellen	Open System Interconnection (OSI) modellen skapades av International Organization for Standardization (ISO) i början av 80-talet för att strukturera implementeringen av protokoll och tjänster i datanätverk. Se bilaga 1 för en utförlig förklaring.
OTEC	Open Communcation for Traffic Engineering Components
Outstations	Gränssnittsområde i OCIT för kommunikation mellan central och fältappart
PDO	Process Data Object, CanOpen
PDU	Protocol Data Unit, data delen av ett meddelande i Modbus
PLC	Programmable Logic Controller
PMPP	Point-to-Multi Point Protocol
PPP	Point-to-Point Protocol
Profibus	Industristandard för kommunikation

Ram	se Header
RS232	Standard för seriell datakommunikation.
RS485	Standard för seriell datakommunikation.
RS485-IS	Standard för seriell datakommunikation.
RSC	Road Side Cabinet, skåp som bl. a. innehåller en övervakningsdator, ett modem och SCU.
RTU	Remote Terminal Unit, definierar bit innehållet hos seriellt överförda meddelanden
SCU	Site Controll Unit har övervakningsfunktioner och sitter i ett RSC
SDU	Service Data Object, CanOpen
SFMP	Simple Fixed Management Protocol, modifikation av SNMP använd i NTCIP
SHA-1	Secure Hash Algoritm, är en typ av hashkodning
SLIP	Serial Line Interface Protocol
SNMP	Simple Network Management Protocol
SRT	Send and Request Data with reply
SRT	Soft Real Time är en optimerad realtids kommunikationskanal
SS	Security Service
SSL	Secure Socket Layer
STMP	Simple Transportation Management Protocol, modifikation av SNMP använd i NTCIP
T2	Transportation Transport Protocol tidigare känt som NULL
T2/NULL	se T2
TCIP	Transit Communications Interface Profiles
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TIC	TrafikInformationsCentral, har som uppgift att ....

TLS	Technische Lieferbedingungen für Streckenstationen, tysk standard
TLV	Type, Length, Value
TMDD	Traffic Management Data Dictionary
TMP	Transportation Managemant Protocol är ett samlingsnamn för SFMP, SNMP och STMP som används i NTCIP
Token	Sätt att avgöra vilken enhet i ett nätverk som har rätt att skicka data.
UDP	User Datagram Protocol
UIC	User Identification Control
Unicast	Ett meddelande skickas till en mottagere
UNIX-Kodering	Tids format som stöds av de flesta operativsystem
Utbytbarhet	I detta sammanhang menas möjligheten till att en apparat från leverantör X med viss funktion (exempelvis styrapparat för trafiksignal) kan bytas till en apparat från leverantör Y med bibehållen funktionalitet.
VIV	Verband ders Ing. Büros für Verkehrstechnik
WAN	Wide Area Network är ett nätverk som sträcker sig över ett stort område, exempelvis ett telenät.
XDR	External Data Representation
XML	Extensible Markup Language är ett nytt språk för www, med många fördelar jämte befintliga språket HTML.

5 Beskrivning av genomförandefasen

Först har kriterier för urval av relevanta protokoll och standarder tagits fram. Detta har skett genom samtal med handledare samt genom vissa litteraturstudier.

Genom samtal och intervjuer med branschfolk och handledare har protokoll och standarder som uppfyller dessa kriterier sökts och funnits. De funna protokollen och standarderna har sedan beskrivits så omfattande som möjligt. Information till dessa beskrivningar har för standarderna inhämtas från respektive standards bakomliggande organisation, detta har främst skett genom omfattande litteratur- och Internetstudier. För de icke standardiserade protokollen har information främst inhämtas från de företag som skapat eller använder protokollen ifråga. Detta har främst skett genom intervjuer av personer med ansvar för detta på företagen samt till viss del genom studier av dokumentation.

De ITS-områden som främst berörs av aktuella protokoll och standarder och har störst utbredning i Sverige har beskrivits. Beskrivningarna har gjorts efter samtal med branschfolk samt genom vissa litteraturstudier.

Under ovanstående samtal och intervjuer framkom en problembild med det skilda bruket av protokoll och standarder i olika system. Denna problembild har utifrån detta beskrivits, ytterligare frågor har ställts till personer med lämplig bakgrund för att komplettera och säkerställa korrektheten i denna problembild.

Under frågeställningen ”Vad bör göras?” diskuteras vad som bör göras för att upphäva de problem som finns beskrivna i problembilden. Enda relevanta åtgärden mot dessa problem är en standardisering. Frågan hurvida en standardisering bör ske diskuteras genom beskrivningar av dess nytta, för- och nackdelar samt ett resonemang kring om tidpunkten är den rätta. Information för dessa beskrivningar och resonemang har inhämtas genom intervjuer och samtal med branschfolk samt genom litteraturstudier.

Under frågeställningen ”Hur bör det göras?” diskuteras hur en standardisering bör ske. Frågeställningen har delats upp i flera delfrågor, dessa delfrågor har besvarats genom självstudier, litteraturstudier, samtal och intervjuer med personer med branschkännedom. För respektive fråga har rekommendationer för vad som är viktigt gjorts.

Med anledning av de rekommendationer som gjorts, har en utvärdering genomförts av aktuella standarder. Denna utvärdering är främst inriktad mot de tekniska rekommendationer som gjorts. Utifrån denna utvärderings resultat har en rekommendation gjorts för vilken standard som är mest lämplig att använda vid en eventuell standardisering.

6 Kriterier för urval

Nedan definieras de kriterier som används för att välja ut relevanta protokoll och standarder.

Ett protokoll är ett regelverk för hur meddelanden och datainnehåll kodas och överförds mellan elektriska apparater. För att kunna kommunicera måste apparaterna i varje ända av överföringen använda samma protokoll. Ett protokoll kan jämföras med ett mänskligt språk där alfabet, vokabulär och grammatik regler användas av alla som talar språket. En standard består av ett protokoll eller en protokollstack och kan ha helt eller delvis definierat datainnehåll.

Det finns ett vitt spektra av tillämpningar inom ITS-området, långtifrån alla berörs av denna rapport. De områden som är aktuella i denna rapport är de som är i behov av respektive kan vara i behov av kommunikation mellan fältapparat och central eller mellan fältapparater. Berörda områden i Sverige med störst utbredning är trafiksignaler, variabla skyltar och Väg Väder informations System (VViS).

För att ett protokoll eller en standard ska tas upp i denna rapport krävs att det är ett protokoll eller en protokollstack som kan används inom något av ovan definierade ITS-områden.

7 Systembeskrivning

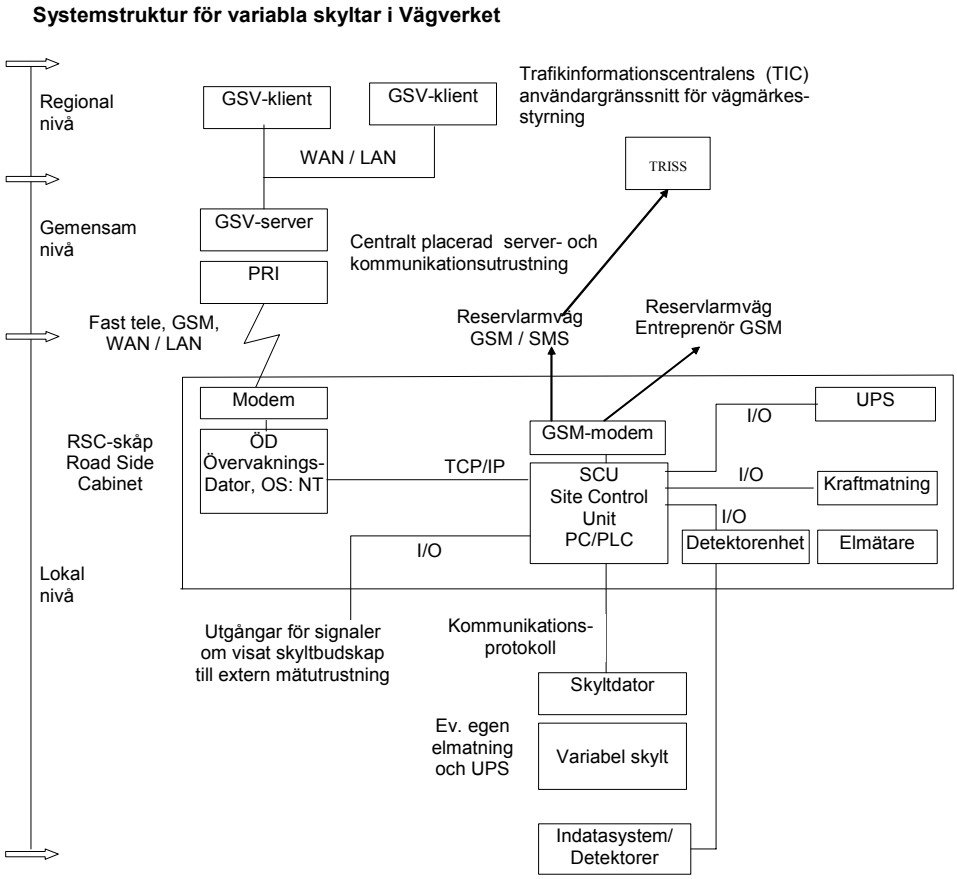
Nedan beskrivs i grova drag befintlig kommunikation till apparater och utrustningar som främst berörs av denna rapport. I kapitel 11 beskrivs världsstandarder med ITS-anknytning, sådana standarder kan omfatta en eller flera av nedan beskrivna områden samt flera andra ITS-områden.

7.1 Variabla skyltar

Kommunikationen till variabla skyltar kan principiellt delas upp i två olika typer av kommunikation, kommunikation till centralt respektive decentralt placerade skyltar. Med kommunikation till decentrala variabla skyltar menas kommunikation till skyltar främst placerade längs landsvägar, där avstånden är stora och kommunikationsinfrastrukturen begränsad. Med kommunikation till centrala variabla skyltar menas främst kommunikation till skyltar placerade i storstäder, där avstånden är små och kommunikationsinfrastruktur finns.

7.1.1 Kommunikation till decentralt placerade variabla skyltar

Nedan beskrivs i ett exempel från en upphandling hur Vägverket styr variabla skyltar i anslutning till en landsväg.



Figur 1 Systemstruktur för kommunikation till variabla skyltar i Vägverket (Källa: Vägverket med vissa förändringar)

Vägverkets trafikinformationscentraler (TIC) styr variabla skyltar genom användargränssnittet GSV-klient. Från en TIC skickas GSV-meddelanden över WAN eller LAN till en GSV-server som finns centralt placerade. Vid GSV-servern finns en modempool, från modempoolen kontaktas ett Road Side Cabinet (RSC-skåp) som befinner sig nära den eller de skyltar som den styr. Denna kommunikation kan ske över bl. a. telenätet, WAN/LAN eller via GSM.

Ett RSC-skåp är ett skåp som innehåller:

- Plats för övervakningsdator som tillhandahålls av Vägverkets IT avdelning
- Plats för telemodem som tillhandahålls av Vägverkets IT avdelning
- Site Controll Unit (SCU), dess uppgifter beskrivs nedan
- Elektrisk utrustning och elmätare
- Kommunikationsgränssnitt

Övervakningsdatorns uppgift är att hantera allt meddelandeutbyte mellan SCU och överordnande system. Detta meddelandeutbyte sker över ett kommunikationsgränssnitt definierat av Vägverket.

SCU:s uppgifter är att:

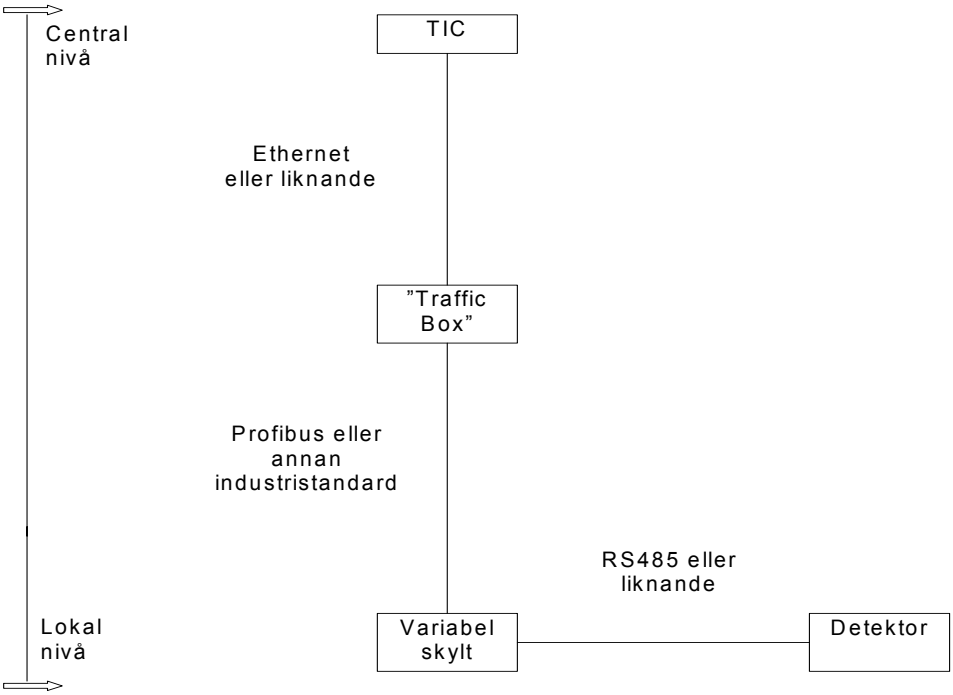
- Övervaka och styra ett eller flera anslutna skyltar
- Övervaka samt samla in och bearbeta data från anslutna indatasystem
- Övervaka egna funktioner
- Övervaka elinfrastrukturen
- Svara för loggning av händelser

SCU innehåller de styralgoritmer som erfordras för styrning av autonoma system.

SCUn övervakar och styr anslutna skyltar genom att kommunicera med det enskilda skyltens dator, kallad skyltdator. Skyltdatorn har till uppgift att hantera vägmärkets status och vägmärkets elinfrastruktur. Kommunikationen mellan SCUn och skyltdatorn sker med hjälp av ett protokoll företaget som tillverkat skylten tillhandahåller. Dessa protokoll beskrivs tillsammans med en del andra icke-standardiserade protokoll för trafiksignaler i kapitel 9.

7.1.2 Kommunikation till centralt placerade variabla skyltar

Kommunikationen till centralt placerade variabla skyltar fungerar principiellt på samma sätt. Skyltarna styrs och/eller övervakas från en TIC. Till (från) TIC: en skickas information från (till) en ”traffic box” över Ethernet, ATM eller liknande nätverk. Från ”traffic boxen” till de variabla skyltarna används en industristandard (exempelvis används Profibus i Stockholm). Detektorer är anslutna till ”traffic boxen” via RS485 (Stockholm). Aktuella industristandarder beskrivs i kapitel 10.



Figur 2 Kommunikation till centralt placerade variabla skyltar

7.2 Trafiksignaler

Vid normala förhållanden kontaktas ca 80 % av en genomsnittlig väghållares trafiksignaler via en kommunikationsslinga, på denna kommunikationsslinga användes ett eget protokoll. Vanligtvis klarar en kommunikationsslinga av ca 10 trafiksignaler så i större städer finns flera kommunikationsslingor. Övriga 20 % är trafiksignaler som befinner sig mer decentralt placerade, dessa trafiksignaler kontaktas med GSM- eller vanliga telemodem.

Den senaste tiden har även andra lösningar börjat komma ut på marknaden, där trafiksignalerna kontaktas med hjälp av någon sorts Digital Subscriber Line (DSL) lösning. Aktuella protokoll beskrivs tillsammans med en del andra icke standardiserade protokoll i kapitel 9.

7.3 Väg Väder informations System (VViS)

Väg Väder informations System (VViS) är Vägverkets system för presentation av vägväderdata. Utmed vägnätet finns 680 stycken VViS stationer utplacerade. Från dessa stationer överförs data som yttemperatur, lufttemperatur, fuktighet, nederbörd och vind till VViS Centralt, där de bearbetas. Överföringen sker via modem över telenätet, centralt placerat finns en modempool som ringer upp respektive stations modem med jämnt tidsintervall. Stationen kan även kontakta modempoolen vid behov (speciella händelser). All kommunikationen sker via telenätet (vanlig telefoni, ISDN samt GSM) gör att det är standardkommunikation som används.

I dagsläget används tre olika typer av dataformat, då det finns 3 olika typer av VViS stationer. Ett utbytningsförfarande pågår så att det inom 2 år endast finns en typ av station kvar och således endast en typ av dataformat.

De standarder som berör överföringar av vägväderdata beskrivs i kapitel 11, där världsstandarder med ITS-anknytning beskrivs.

8 Problembild

I de olika system som beskrivs ovan används i dagsläget en mängd olika protokoll, det är vanligt att en leverantör använder sig av flera protokoll.

Generellt sett tillhandahåller de befintliga protokollen önskade funktioner, då detta regleras vid upphandling av systemen. Vissa problem finns i och med att vissa av de befintliga protokoll som används är utvecklade för andra ändamål, så som styrning av reklamskyltar. Detta medför att viss funktionalitet kan saknas, exempelvis möjligheten att kontrollera vad skylten visar. Detta kan delvis lösas genom att kontrollera vad som valdes att visas senast en ändring skede, men det går inte att kontrollera att det verkligen är det som visas.

Denna avsaknad av funktionalitet är generellt sett inte ett problem, problemet är att apparater som stödjer olika typer av protokoll inte kan kommunicera med varandra och att de i de flesta fall inte kan använda sig av samma kommunikationsnätverk. Att apparater stödjer samma protokoll betyder inte automatiskt att de kan kommunicera med varandra, för att kunna kommunicera med varandra måste de även kunna förstå varandras meddelanden. För att förstå varandras meddelanden måste datainnehållet vara beskrivet på samma sätt. I dagsläget används olika beskrivningar av datainnehållet i Sverige. Dessa problem kan kallas avsaknad av interoperabilitet[1] och utbytbarhet[2]. Avsaknad av interoperabilitet och utbytbarhet leder till sämre konkurrens och risk för monopolbildning.

Problem finns även med utdata från systemen. Normalt aggregeras utdata från systemen med tanke på systemets behov, detta gör att mycket värdefull utdata förloras. Denna förlorade data skulle vara önskevärd att använda i andra sammanhang.

Dessa problem är önskvärda att upphäva, mer om detta nedan i kapitel 12.

[1] Interoperabilitet, förmågan att en mångfald av apparater, oftast av olika typ, problemfritt kan verka tillsammans i ett system med gemensamt ändamål, exempelvis använda samma kommunikationskanal.
[2] Utbytbarhet, i detta sammanhang menas möjligheten till att en apparat från leverantör X med viss funktion (exempelvis styrapparat för trafiksignal) kan bytas till en apparat från leverantör Y med bibehållen funktionalitet.

9 Icke standardiserade protokoll använda i Sverige

Nedan beskrivna protokoll används i Sverige. De är i flera fall framtagna av mindre företag för användning inom flera olika områden. På grund av företagssekretess är informationen i flera fall bristfällig och viktiga uppgifter saknas. Informationen är i samtliga fall hämtade från respektive företag och på grund av det kan eventuella brister ha undanhållits och informationen är mer eller mindre partisk. Ett företag (Stunt AB) vill inte lämna ut några uppgifter alls om sitt protokoll. Eventuellt kan något protokoll som används ha förbisetts, men detta medför inget problem för denna rapports resultat.

9.1 501

Allmänt

501 är utvecklat under 70-talet av Ericsson och är anpassad efter den tidens teknologi. Från början är protokollet utvecklat för att kommunikation mellan en huvudkontrollerare åtta signalkontrollerare. I originalutförande kan protokollet överföra indikationer åt signalkontrollerare från 24 signalgrupper och 32 detektorer. Det går att använda detektorindikatorerna till alternativa ändamål.

Logik

Kommunikationen indikeras varannan sekund genom att ett 2-bytes meddelande skickas ut till signalkontrolleraren. Kontrolleraren svarar med att skicka 9-bytes som innehåller information om kontrollerar status, gruppsignaleringsindikatorer och detektor aktiviteter.

Funktioner

De funktioner som 501 tillhandahåller är övervakning och samordning. Saknas gör fjärrprogrammering, klocka och trafikräkning.

Användning

501 används i styrapparater från K&L, Siemens, Falco och Ericsson (JCF).

Tillgänglighet

501 är Peek Traffic AB: s egendom men är frisläppt.

9.2 601

Allmänt

Utvecklat av Ericsson.

Funktioner

De funktioner som 601 erbjuder är övervakning, samordning, klocka, fjärrprogrammering och trafikräkning.

Användning

601 finns installerat i styrapparater från Ericsson (JCF).

Tillgänglighet

601 är Peek Traffic AB: s egendom och dokumentation fås efter avtal.

9.3 Focus Neons Protokoll

Allmänt

Protokollet togs fram under mitten av 80-talet av Focus Neon, men utveckling sker fortlöpande. Initialt var protokollet framtaget för kommunikation mellan PC-datorer med seriellkommunikation.

Logik

Protokollet är ett master/slav protokoll. Slaven kan endast svara på meddelanden. Hur meddelandet master skickar ser ut beror på vad som skickas. Vid en status fråga är meddelandet endast några bytes, medan det vid överföring av en bild kan röra sig om kilobytes. Slaven däremot svarar jämt med 12 bytes.

Säkerhet

Begränsad tillgång av information över protokollet och en provsumma som säkerställer att data inte ändrats under överföringen.

Användning

Används av Focus Neon i deras produkter, i denna rapport berörda områden är variabla skyltar och parkeringssystem.

9.4 FurturitCom Chain Driver Protocol (ChainCom)

Allmänt

ChainCom är ett protokoll som är framtaget av Swarco Futurit och används för överföringar av data, från ett centralt system till display enheter. Fysiskt överförs data av modem användande fasta eller uppringda linjer, eller i ett nätverk. Data format så väl som kommunikationshastighet är inte begränsade av protokollet.

Logik

ChainCom är ett master/slav protokoll. Det kan endast finnas en master åt gången och endast mastern kan initiera kommunikation. Efter att ha överfört ett meddelande väntar mastern på ett svarsmeddelande. Om inget svar mottagits efter 3 sekunder ser mastern överföringen som misslyckad och försöker igen eller fortsätter med nästa meddelande. En slav kan svara med ett acknowledge (bekräftelse, ACK) eller ett not acknowledge (icke bekräftelse, NACK).

Om ett fel upptäcks i ett mottaget meddelande, skickar inte slaven något svarsmeddelande. Om meddelande har korrekt utformning men ogiltig data svarar slaven med ett NACK meddelande.

Meddelandeuppbyggnad

ChainComs meddelande består av följande:

- Sync (2 byte, $5A + $A5).
- Adress byte, 1-250 är slavadresser, 251-255 är reserverade, där 255 används för Broadcasting av sync blink tid till alla slavar. Slaven svarar med sin egen adress.
- Count (2 bytes), antal data bytes.
- Tag/Cmd (1 byte), de första fyra bitarna används för tag och resterande som kommando. Tagen används för att identifiera ett meddelande. I varje nytt master meddelande inkrementeras tagen. Slaven svarar med samma tag som den fått. Central systemet måste kontrollera att den får tillbaka förväntad tag, annars är meddelandet ogiltigt. I ett master meddelande är alltid kommandot 0. I svarsmeddelanden från slavar är kommandot antingen 1 (ACK) eller 2 (NACK).
- Status (0-2 bytes), används aldrig av mastern. Slaven skickar alltid 2 bytes med statusinformation.
- Chk1 (byte 1), provsumma 1 för alla tidig
- are byte.
- Data (0-65535 byte). Projekt specifik information.

- Chk2 (1 byte), provsumma 2 för alla data byte, finns endast om antalet databyte överstiger 0.

Säkerhet

Provsummor används för att kontrollera att data inte ändrats under överföringen.

Användning

Används i produkter från Swarco.

9.5 Lnet/fdx

Funktioner

De funktioner som Lnet/fdx tillhandahåller är övervakning, klocka, fjärrprogrammering (ELC-panel), trafikräkning och Trats/Traps-information. Saknas gör samordnad styrning av grupper

Användning

Lnet/fdx finns installerat i styrapparater från Peek Traffic.

Tillgänglighet

Lnet/fdx är Softman AB: s (upphört) egendom och licensiering krävs.

9.6 P-Link

Allmänt

Utvecklat av Ericsson.

Funktioner

De funktioner som P-Link tillhandahåller är övervakning, klocka, fjärrprogrammering (ELC-panel), trafikräkning och Trats/Traps-information. Saknas gör samordnad styrning av grupper.

Användning

P-Link finns installerat i styrapparater från Peek Traffic.

Tillgänglighet

P-Link är Peek Traffic AB: s egendom och dokumentation fås efter avtal.

9.7 Safe Traffics Protokoll

Allmänt

Safe Traffics protokoll är utvecklat för att kunna ändra parametrar i Safe Traffics produkter, produkterna varierar mycket till funktion, storlek samt teknik.

Logik

Först ska användaren logga in med hjälp av ett inloggningsblock som innehåller lösenord. Lösenordet är lika för alla produkter av en typ samt innehåller (om aktiverat) ett serienummer. Är inte inloggningsblocket korrekt kommer inget svar, utan totalt tystnad råder från den anropade produkten. Detta för att försvåra för hackers och dylikt.

Är inloggningsblocket korrekt besvaras det med ett ACK, om det vid ett senare tillfälle skickas ett icke korrekt inloggningsblock stängs kommunikationen ner direkt. När kommunikation är öppen och ingen kommunikation pågår stängs kommunikationen efter 5 minuter och en nu inloggning måste ske.

Godkända block besvaras med antingen ett ACK eller ett datablock om produkten ska svara med data.

Meddelandeuppbyggnad

Varje meddelande innehåller följande:

- STX
- Funktion, exempelvis hastighet, text eller parameter
- Subfunktion, exempelvis Läs (till produkt), Skicka (från produkt), Antal och Radera
- Optional1
- Optional2 (data)
- Provsumma
- ETX

Funktioner

Protokollet används för att ändra texter, parametrar, reaktionssätt och övriga styrningsegenskaper. Det används även för att hämta aktuell data från produkterna.

Säkerhet

Vid fel provsumma eller vid data som ej är ASCII-format förkastas blocket och ett NACK skickas. Se även under Logik där ett säkerhetsrelaterat inloggningsförfarande beskrivs.

Användning

Används i Safe Traffics produkter, produkter med ITS koppling är variabla skyltar och Du-Kör-För-Fort-skyltar.

9.8 STCIP

Allmänt

STCIP är framtaget av Peek Traffic och är en anpassning av NTCIP (se kapitel 11) för Skandinavien.

Omfattning

STCIP omfattar center till apparat kommunikation och nyttjar UDP/TCP, IP och SNMP. Det stödjer övervakning av apparater (status, fel), datainsamling (trafikdata, signalgruppsdiagram), order till apparater (Driftform, tidplan) och fjärrprogrammering (apparatberoende). Samordningsfunktioner omfattas ej (görs via 501).

Användning

STCIP finns installerat i Peek Traffic: s styr- och övervakningsgsystem OmniVue i bland annat Malmö och Oslo.

Tillgänglighet

Öppet för alla som vill utveckla egna gränssnitt. Peek Traffic ansvarar för innehåll och administration. Peek Traffic svarar för support, testning och verifiering. För ”medlemskap” och tillgång till support tar Peek Traffic ut en inträdeskostnad.

10 Relevanta världsstandarder från produktionsindustrin

Nedan beskrivs summariskt världsstandarder från produktionsindustrin som inom ITS-området främst används för styrning av variabla skyltar, fullständiga beskrivningar finns i bilaga 2. Informationen om standarderna har inhämtas från respektive standards bakomliggande organisation, på grund av detta är informationen mer eller mindre partisk och brister kan ha undanhållits.

Standardernas tillgänglighet som nämns nedan är vad som gäller vid användning av standarderna som de är. Vad som gäller om standarderna vidareutvecklas är oklart.

10.1 CANopen

CANopen är ett standardiserat applikationsskiktsprotokoll optimerat för inneslutna nätverk (främst Controller Area Network, CAN). Huvudsakligen används det i inneslutna låg- och medelvolymssystem, men det finns även implementerat i automatiseringskontrollsystem. I de lägre skikten används CAN protokollet.

10.1.1 Omfattning

CANopens specifikationer täcker applikationsskikt och kommunikationsprofil, så väl som struktur för programmerbara apparater, rekommendationer för kablar, kontakter för SI enheter och prefix representationer.

10.1.2 Medverkande

CANopen och CAN är framtaget av CAN in Automation (CiA) som är användare och leverantörers internationella organisation, i dagsläget har CiA 565 medlemmar. CiA utvecklar och stödjer CAN-baserade protokoll ur de högre skikten i OSI-modellen. Alla aktiviteter är baserade på CiA medlemmars intresse, deltagande och initiativ. CiA representanter stödjer aktivt standardisering av CAN protokoll och representerar medlemmarnas intressen i nationella och internationella standardiseringsorganisationer, som ISO och IEC. Medlemmarna i CiA initierar och utvecklar specifikationer som sedan publiceras som CiA standarder. Dessa specifikationer täcker fysiska skiktets definitioner såväl som applikationsskiktets och utrustningsprofilbeskrivningar.

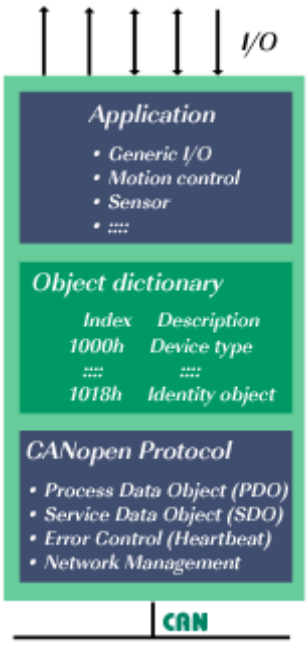
10.1.3 Kommunikationsmodell

Alla CANopen apparater kan ses på samma sätt, apparaterna är anslutna till CAN på ena sidan och till applikationsspecifika I/O data på den andra sidan (se figur 4). Gränssnittet mellan applikation och CAN är realiserat av ett objektlexikon. Objektlexikonet är unikt för varje CANopen apparat och representerar hela accessen till dess implementerade applikation i form

av data och konfiguration. För att få access till objektlexikonet måste varje CANopen apparat realisera en CANopen protokollstack. Denna CANopen protokollstack är en del av mjukvaran, som normalt är implementerad i samma kontrollerare som används av applikationsmjukvaran.

CANopen protokollstacken består av olika funktioner för olika ändamål.

- Process Data Object (PDO) används för att överföra applikationsdata. Applikationsdata överförs utan någon protokollheader (frame) i Broadcast.
- Service Data Object (SDO) används för att få access till en apparats alla parametrar och för direkt apparat till apparat kommunikation.
- Felkontroll används för att validera att alla apparater fungerar ordentligt vad gäller dess CANopen kommunikation.
- Nätverksmanagement används för att kontrollera nätverket vad gäller CANopen kommunikation och indirekt i form av systemuppförande.



Figur 3 CANopen kommunikationsmodell (Källa: www.canopen.org)

10.1.4 Användning

CANopen används inom en mängd olika tillämpningsområden. Huvudområdena är följande:

- Lastbilsbaserade överbyggnadskontrollsystem
- Anläggningsmaskiner
- Passagerar- och godståg
- Marinelektronik
- Fabriksautomatisering
- Industriell maskinkontroll
- Hissar och rulltrapport
- Byggnadsautomatisering
- Medicinsk utrustning

- Icke industri kontroll
- Icke industri utrustning

CAN kan användas i alla ovan nämnda områden samt inom följande områden:

- Passagerarfordon
- Lastbilar och bussar
- Flyg- och rymdelektronik

Inom denna rapports berörda ITS-områden används det av det tyska företaget Niechoj electronic GmbH. Niechojs produkter marknadsförs och säljs i Sverige av Lumilite AB.

10.1.5 Tillgänglighet

För tillgång till CiAs standarder krävs medlemskap i CiA. Medlemskap fås mot en medlemsavgift som betalas årsvis. Kostnaden för detta medlemskap varierar från 180 euro för associerade medlemmar (studenter) till 7 500 euro för företag med mer än 100 000 anställda.

10.2 Modbus

Modbus är en industristandard med ursprung från 70-talet. Den används främst för kommunikation mellan automatiseringsutrustningar. Modbus tillhandahåller klient/tjänare kommunikation mellan utrustningar anslutna till olika typer av bussar och nätverk.

10.2.1 Omfattning

Modbus protokollet erbjuder en enkel kommunikation i alla typer av nätverksarkitekturer. Alla typer av anordningar (PLC, HMI, kontrollbord, händelse kontroll, I/O utrustning, m.m.) kan använda Modbus protokollet för att initiera operationer. Kommunikation med hjälp av Modbus kan ske seriellt med master/slav, med TCP/IP på ett Ethernet nätverk eller på ett höghastighetsnätverk med en token.

10.2.2 Medverkande

Modbus styrs av en organisation med namnet Modbus. Medlemmar i organisationen är användare och leverantörer av Modbusbaserade utrustningar. I dagsläget finns ca 330 företag registrerade som användare av Modbus.

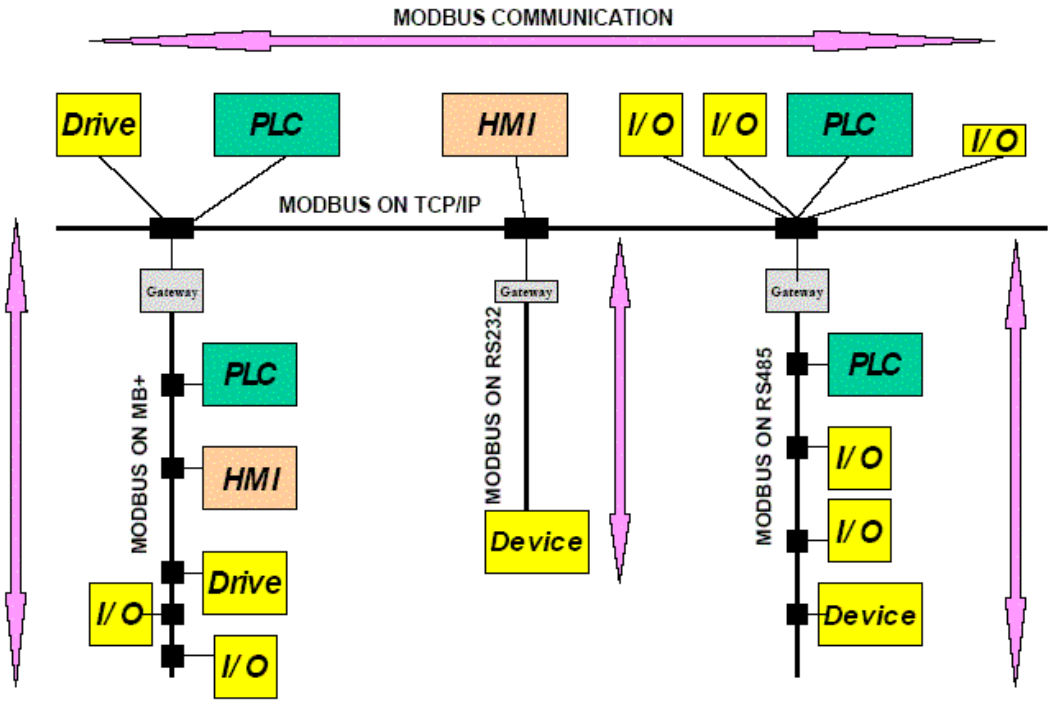
10.2.3 Kommunikationsmodell

Modbus protokollet tillhör skikt 7 i OSI-modellen. Som tidigare nämnts kan Modbus kommunikation ske på flera olika sätt. I tabell 1 finns en sammanställning över de tre kommunikationssätten och deras protokollstackar. Modbus med seriell kommunikation och Modbus med TCP/IP på Ethernet beskrivs mer ingående nedan.

OSI-skikt	Modbus med seriell kommunikation	Modbus med TCP/IP på Ethernet	Modbus med token
7	Modbus	Modbus	Modbus
6	Inget	Modbus on TCP	Inget
5			
4		TCP	
3		IP	
2	Modbus Serial Line Protocol	Ethernet	Modbus+ / HDLC
1	EIA/TIA-485 alt. EIA/TIA-232	Valbart	Valbart

Tabell 1 Sammanställning av protokoll i Modbus beroende underliggande skikt

De olika protokollstackarna hindrar inte kommunikation mellan utrustningar anslutna via olika protokollstackar, de olika utrustningarna kommunicerar med hjälp av Gateways.



Figur 4 Exempel på Modbus kommunikation vid olika protokollstackar (Källa: Modbus Application Protocol Specification V1.1 med vissa förändringar)

10.2.4 Användning

Modbus används främst för industriell kommunikation och automatisering. Inom denna rapports berörda ITS-områden används det av det tyska företaget Niechoj electronic GmbH. Niechojs produkter marknadsförs och säljs i Sverige av Lumilite AB.

10.2.5 Tillgänglighet

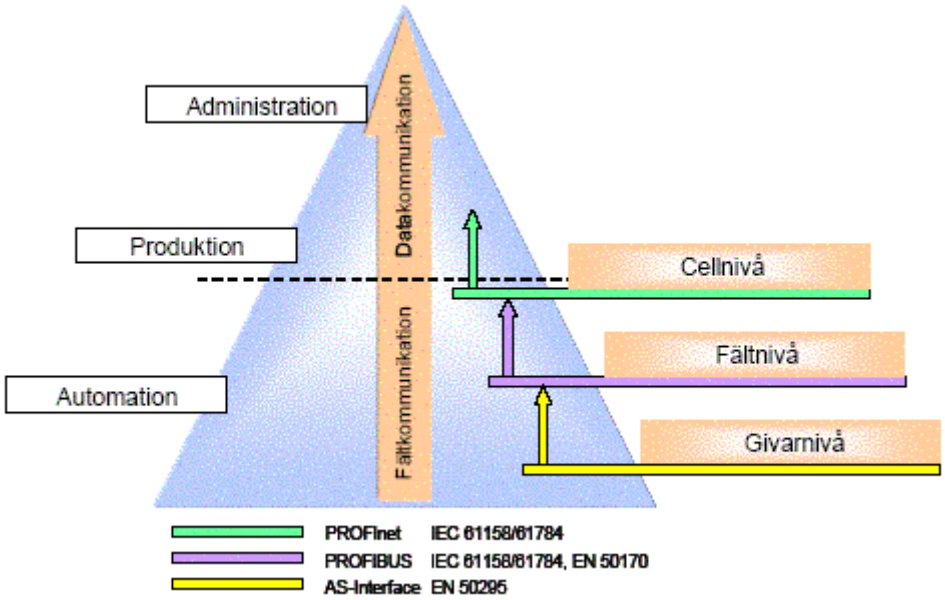
Det finns olika typer av medlemskap med skilda kostnader beroende på företagsstorlek och intresse.

10.3 Profibus

Profibus är ett öppet enhetligt digitalt kommunikationssystem som kan användas i så gott som alla automationsområden, i verkstadsindustrin och processautomation i synnerhet men även i trafikstyrning, kraftproduktion och –distribution. Profibus kommunikation är förankrad i de internationella standarderna IEC 61158 och IEC 61784.

10.3.1 Omfattning

Profibus erbjuder kommunikation för alla verkstads- och processautomation. I figur 5 ses en översikt över kommunikationen i automationsteknologi.



Figur 5 Kommunikation i automationsteknologi (Källa: Profibus Teknologi och användning)

På givarnivå överförs signaler från digitala givare och aktorer på en givarbuss. Lämpligt är en buss med enkel installationsteknik där både strömförsörjning och data överförs. I Profibus används AS-Interface som lämpar sig väl för detta ändamål. För information om AS-Interface hänvisas till facklitteratur.

På fältnivå behövs realtidskommunikation mellan fältenheter, som I/O moduler, transmittrar, drivutrustning, analysinstrument, ventiler och operatörspaneler, och automationssystem. Data ska överföras såväl cykliskt som acykliskt. I Profibus används standarden Profibus för detta ändamål. Profibus beskrivs till fullo i bilaga 2.

På cellnivå kommunicerar PLC: er och industriPC med varandra och med IT-system i kontorsvärlden. Denna kommunikation sker med standarder som Ethernet, TCP/IP, Intranät och Internet. Informationsflödet kräver stora datapaket och en uppsättning kraftfulla kommunikationsfunktioner. För detta ändamål har Profibus utvecklat det öppna och tillverkaroberoende automationskoncept som är baserat på Ethernet. PROFInet beskrivs till fullo i bilaga 2.

10.3.2 Medverkande

Profibus International som står bakom Profibus är världens största organisation för industriell kommunikation. I dagsläget har organisationen ca 1400 medlemmar. Medlemmar i organisationen kan vara försäljare av hårdvara, mjukvara och system så väl som användare och operatörer, vetenskapliga institut och federationer. Det finns regionala Profibus organisationer i 23 länder, 21 ackrediterade kompetenscentrum och 7 testlaboratorier för certifieringsarbete.

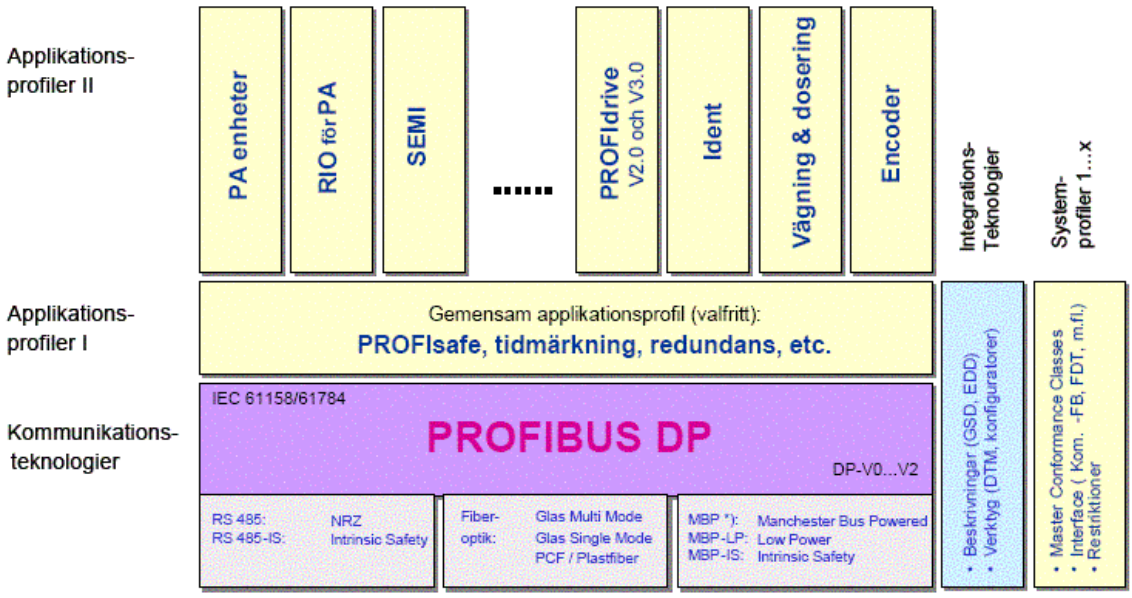
Profibus Internationals huvudsakliga uppgifter är följande:

- Underhålla och utveckla Profibus teknologin
- Utöka acceptansen och användningen av Profibus teknologin
- Skydda användarnas och tillverkarnas investeringar genom att påverka och delta i fortsatt standardisering
- Representera medlemmarnas intresse genom att vara remissinstans för standardiseringskommittéer och organisationer
- Ge teknisksupport över hela världen
- Skapa kvalitetsgaranti genom produktcertifiering

Utvecklingen av Profibus teknologin har överlåtits av Profibus International till den regionala organisationen i Tyskland. Utvecklingsarbetet är organiserat i 5 tekniska kommittéer med mer än 35 permanenta arbetsgrupper. Dessutom finns ett antal extra arbetsgrupper som handhar speciella tidsbegränsade uppgifter. Arbetsgrupperna tar fram specifikationer och profiler, handhar kvalitetsarbetet och standardiseringen, arbetar i standardiseringskommittéer och utför marknadsaktiviteter (mässor, presentationer) för att få Profibus teknologin att växa.

10.3.3 Profibus Kommunikationsmodell

I Profibus standardiseras OSI-modellens skikt 1,2 och 7, i övriga skikt används inga protokoll. Ovanför skikt 7 finns olika typer av profiler, allmänna applikationsprofiler, speciella applikationsprofiler och systemprofiler. Applikationsprofilerna är utformade för specifika produktgrupper och användningsområden. Systemprofilerna beskriver systemklasser, vilket inkluderar funktion, programgränssnitt och hur de ska integreras. I figur 6 ses Profibus systemuppbyggnad för protokoll och applikationsprofiler.



Figur 6 Teknisk systemuppbyggnad för Profibus, applikationsprofiler I är allmänna applikationsprofiler och applikationsprofiler II är speciella applikationsprofiler (Källa: Profibus Teknologi och användning)

10.3.4 Tillgänglighet

Det finns olika typer av medlemskap med skilda kostnader (från 1200 kr till 30 000 kr per år) beroende på företagsstorlek och intresse.

10.3.5 Användning

Profibus används främst inom ITS för styrning av variabla skyltar, bland annat används Profibus i MTM-systemet i Stockholm.

11 Världsstandarder med ITS-anknytning

Nedan beskrivs summariskt relevanta världsstandarder med ITS-anknytning, fullständiga beskrivningar finns i bilaga 3. Dessa standarder täcker med skild grad berörda ITS-områden. Informationen om respektive standard har inhämtas från respektive standards bakomliggande organisation, på grund av detta är informationen mer eller mindre partisk och brister kan ha undanhållits.

Standardernas tillgänglighet som nämns nedan är vad som gäller vid användning av standarderna som de är. Vad som gäller om standarderna vidareutvecklas är oklart.

11.1 IVERA

IVERA är ett holländskt protokoll som tagits fram för att tillhandahålla en tillverkaroberoende lösning för kommunikation mellan kontrollcentraler och trafiksignaler. Protokollet kan även användas i andra kommunikationssystem. Namnet IVERA är en kombination av förkortningarna för Initiatiefgroep VErkeersregeltechnici Rijkswaterstaat en Provincies (IVER, Initiative Group of Traffic Control Engineers of Department of Public Works and Provinces) och ASsociation of TRaffic Industries in the Netherlands (ASTIN) som är två av de bakomliggande organisationerna.

11.1.1 Omfattning

Initialt har IVERA protokollet blivit utvecklat för kommunikation mellan trafiksignaler och en kontrollcentral. I tillägg till det passar IVERA protokollet för applikationer som:

- Kommunikation med system för påfartskontroll
- Kontroll av skyltar i parkeringssystem
- För sammanlänkning av kontrollcentraler

I designen av IVERA protokollet är utgångspunkten ett maximalt användande av standard kommunikationsinrättningar för både kommunikationsinfrastruktur och –mjukvara. Fördelar med detta är:

- Stöd av olika kommunikationsnätverk som telefonnätet och punkt till punkt kabel kommunikationer
- Stöd av befintliga protokoll
- Tillverkaroberoende lösningar
- Minimal utvecklingsansträngning genom användande av standard hårdvaru- och mjukvarukomponenter

11.1.2 Medverkande

Initiativtagare till IVERA protokollet är ASTIN, Commissie Verkeersregeltechnici Nederland (CVN, Committee of Traffic Control Engineers in The Netherlands) och IVER.

ASTIN är en organisation för holländska bolag som arbetar med trafikteknik. Medlemmar är Peek Traffic, Siemens Nederland, TPA Traffic and Parking Automation och Vialis Verkeer en Mobiliteit. CVN är en kommitté för trafiksignalingenjörer i Holland. IVER är en sammanslutning bestående av Hollands fyra största städer.

En arbetsgrupp bestående av delegater från IVER och ASTRIN är ansvariga för genomförandet av IVERA. Arbetsgruppens uppgift är ett skriva en funktionell specifikation för kommunikation mellan ett centralt system och trafiksignaler.

Protokollet ägs av stiftelsen Beheer ASTRIN/IVERA protocol.

11.1.3 Kommunikationsmodell

IVERA protokollet tillhör skikt 7 i OSI-modellen. IVERA protokollet kommunicerar med underliggande nätverksskikt via standardfunktioner (stream eller fil I/O). IVERA protokollet gör följande antaganden med avseende på underliggande skikt:

- Underliggande skikt tillhandahåller skapande och underhåll av en förbindelseorienterad förbindelse mellan IVERA master och IVERA slav. En möjlig implementering för en sådan förbindelse är en förbindelse baserad på TCP/IP.
- Underliggande skikt säkerställer att de byte som skickas av IVERA mastern anländer felfritt och i samma ordning till IVERA slaven och vice versa.
- Underliggande skikt tillhandahåller segmentering och routing.
- I de fall när mer än en logisk förbindelse finns mellan kontrollcentral och trafiksignaler över samma fysiska förbindelse har IVERA meddelanden prioritet.
- Om datakomprimering krävs eller är nödvändig så ska den implementeras i lägre skikt.
- Om datakryptering krävs ska den implementeras i lägre skikt.

IVERA protokollet fungerar över TCP/IP och PPP, för vilket lösningar kan certifieras hos stiftelsen Beheer ASTRIN/IVERA protocol. Eventuellt kommer det även att fungera direkt över en fysikförbindelse.

11.1.4 Användning

IVERA protokollet används i Holland av företagen Peek Traffic, Siemens Nederland, TPA Trafic en Parking Automation, Vialis Verkeer en Mobiliteit och Ko Hartog. I dagsläget finns protokollet installerat i ca 400 trafikledningsinstallationer, antalet växer kontinuerligt.

11.1.5 Tillgänglighet

För användning av IVERA protokollet utfärdar stiftelsen ”Beheer ASTRIN/IVERA protocol” licenser.

11.2 National Transportation Communications for ITS Protocol (NTCIP)

National Transportation Communications for ITS Protocol (NTCIP) är en familj av standarder för överföring av data och meddelanden mellan kontrollsystem och apparaterr använda inom ITS. Det är baserat på datakommunikationsstandarder.

11.2.1 Omfattning

NTCIP: s standarder är tänkta att kunna användas i alla sorters ledningssystem som hanterar något inom trafikmiljön, exempelvis de för motorvägar, trafiksignaler, räddningsledning, transittrafik, resandeinformation och dataarkivering. Det är tänkt att användas för fast och trådlös kommunikation mellan datorer i olika system eller ledningscentraler och datorer eller apparater efter vägar.

NTCIP omfattar ej standarder för:

- Kommunikation mellan fältapparater och fordon. Kommunikation mellan fältapparater och centrals stöds.
- Överföring av videobilder i full upplösning. Överföring av videokamerans kontrolldata och ändringskontrolldata stöds genom användning av en separat kommunikationskanal.
- Överföring av resandeinformation till privat ägda fordon. Här inkluderas speciella Broadcasting och begränsade bandbredds protokoll som arbetar i samarbete med FM radiostandarder och mobilradio. Överföring av information från olika källor till resandeinformationscentralen stöds.
- Kommunikation för finansiella transaktioner
- Fordonsintern kommunikation för exempelvis avancerad fordonskontroll och säkerhet.
- Kommunikation mellan styrapparat och annan elektronisk utrustning i RSC-skåp.

11.2.2 Medverkande i NTCIP

För att säkerställa både leverantörers, användare och regeringens (USA:s regering) stöd, så är NTCIP ett samarbete mellan National Electronics Manufacturers Association (NEMA), American Association of State Highway and Transportation Officials (AASHTO) och Institute of Transportation Engineers (ITE) med ekonomiskt stöd från Federal Highway Administration (FHWA). De olika organisationerna har inga speciella roller i NTCIP utan arbetet styrs av en kommitté, där de tre organisationerna har sex medlemmar vardera.

11.2.3 Protokoll i NTCIP

NTCIP tillhandahåller standarder för två olika typer av ITS kommunikationer. Den första typen är kommunikation mellan ledningssystem eller centraler och multipla kontroll- eller övervakningsutrustningar som styrs av systemet eller centralen. Då de flesta av dessa system

involverar en dator eller ett ledningssystem som kommunicerar med olika typer av apparater efter vägkanter och verksamhetsfordon kallas denna typ av kommunikation för ”center-to-field” (C2F, central-till-fält). Exempel på C2F system är variabla skyltar, trafiksignaler, fordonsdetektorer och vädersensorer.

Den andra typen är kommunikation mellan centrala ledningssystem. Denna typ av kommunikation kallas ”center-to-center” (C2C, central-till-central). Exempel på C2C system är trafikledningssystem, parkeringsledningssystem, olycksledningssystem och reseinformation.

Bägge dessa kommunikationstyper har en delvis gemensam kommunikationsmodell med protokoll som beskrivs nedan.

11.2.4 Kommunikationsmodell

NTCIP använder sig av en skiktmodell som liknar OSI-modellen. Istället för OSI-modellens sju skikt innehåller NTCIP: s modell fem skikt, informationsskiktet, applikationsskiktet, transportskiktet, subnätverksskiktet och anläggningsskiktet.

Informationsskiktets standarder definierar innebörden av data och meddelanden och den generella hanteringen av ITS information. Skiktet är ovanför OSI-modellens högsta skikt och således saknas motsvarande skikt i OSI-modellen.

Applikationsskiktets standarder definierar regler och procedurer för överföring av informationsdata. Det motsvaras i stort av applikations-, presentations- och sessionskiktet i OSI-modellen.

Transportskiktets standarder definierar regler och procedurer för överföring av applikations data från punkt ”X” till punkt ”Y” i ett nätverk, inkluderat är routing, meddelande hopsättning/isärtagning och nätverksmanagement funktioner. I OSI-modellen motsvaras det i stort av transport- och nätverksskiktet.

Subnätverksskiktets standarder definierar regler och procedurer för överföring av data mellan två ”intilliggande” apparater över något kommunikationsmedium. Det motsvaras i stort av datalänk- och fysiska skiktet i OSI-modellen.

I anläggningsskiktet bestäms vilken kommunikationsinfrastruktur som används för kommunikationen. Att notera är att anläggningsskiktet inte är ett val av standard utan ett val av infrastruktur, vilket påverkar valet av standard i subnätverksskiktet. Motsvarande skiktet saknas i OSI-modellen.

OSI-modellen	NTCIP-modellen
	Informationsskiktet (1)
Applikationsskiktet (7)	Applikationsskiktet (2)
Presentationsskiktet (6)	
Sessionskiktet (5)	
Transportskiktet (4)	Transportskiktet (3)
Nätverksskiktet (3)	
Datalänk skiktet (2)	Subnätverksskiktet (4)
Fysiska skiktet (1)	
	Anläggningsskiktet (5)

Tabell 2 OSI-modellens skikt jämförda med NTCIP-modellens skikt

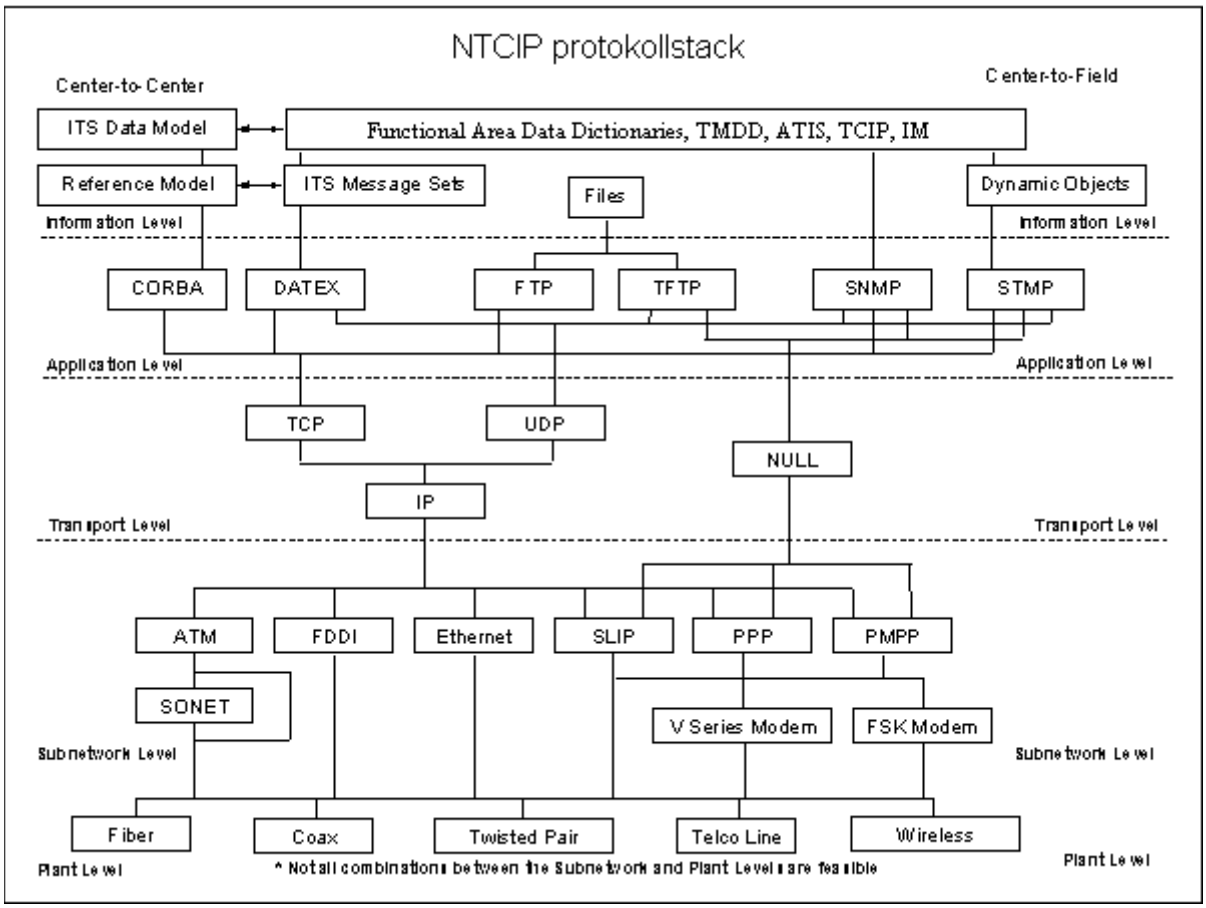
Informationsskiktets standarder som används inom ITS är unika för transportindustrin. Mycket av den pågående standardiseringsansträngningen inom ITS involverar identifikation av obligatoriska dataelement och definition av deras användning för olika domäner och funktioner inom ITS.

På applikations-, transport- och subnätverksskiktet nivå kan ITS i stort sett använda sig av befintliga telekommunikationsstandarder. NTCIP specificerar vilka optioner som ska användas ur en standard när det finns flera alternativ.

NTCIP har utökat befintliga standarder eller utvecklat nya protokoll som behövs i fall där ITS har speciella behov. De två områden där ITS främst har speciella kommunikationskrav är:

- Kontinuerliga, automatiserade, realtidsöverföringar av stora volymer av små datapaket i många-till-många multiförmedlingsnätverk.
- Kontinuerliga höga volymer av realtidsdata skickade till och från processorer vid vägkanter eller fordonsutrustningar som delar samma låghastighetsdatakanal och har krav på låg latens (konstant överföringstids fördröjning).

I NTCIP kan en mängd olika protokoll/standarder användas i respektive skikt. I figur 7 ses en sammanställning över NTCIP: s struktur. Figuren visar de olika protokoll (rutor) som kan användas i respektive skikt och vilka som är kompatibla med varandra (linjer som sammanbinder rutorna). Inte alla kompatibla konfigurationer är användbara fast de är möjliga. Exempelvis så är inte vanligt att använda Simple Network Management Protocol (SNMP), ihop med TCP/IP.



Figur 7 NTCIP: s protokollstack (källa http://www.ntcip.org/library/protocols/ med vissa förändringar)

11.2.5 Användning

NTCIP används i dagsläget i USA, oklart om samtliga tänkbara applikationer används.

11.2.6 Tillgänglighet

NTCIP är fritt att använda.

11.3 Open Communication Interface for Road Traffic Control Systems (OCIT)

Open Communication Interface for Road Traffic Control Systems (OCIT) är en tysk arbetsgemenskap för standardisering inom området vägtrafikteknik. OCIT: s arkitektur fokuserar på Intelligenta Transport System (ITS), i förstahand med inriktning mot trafiksignaler, men det är även inriktat mot andra områden som trafikdetektorer och variabla skyltar.

11.3.1 Omfattning

OCIT: s ledtankar är för standardisering är:

- Standardiserade och öppna gränssnitt är en förutsättning för fabrikatsblandade system och således mer konkurrens
- Trots standardisering måste utrymme för konkurrens finnas, som förutsättning för innovations- och prestationsförmåga för trafikteknik
- Standardiseringsansträngningen baseras på regler och systemarkitektur för vägtrafikteknik som finns i Tyskland, Österrike och Schweiz, men har som mål att få internationell utbredning.

Dessa ledtankar gör att målet för OCIT: s standardisering är att åstadkomma kommunikationsgränssnitt för fabrikatsblandade system. Gränssnitten är de mellan komponenter, apparater och system. Standardiserat blir protokoll, funktioner och data som betjänas i gränssnitten. Inre egenskaper som systemuppbyggnad, applikationer och databaser som inte hänger samman med gränssnitten omfattas ej av OCIT: s arbete. Detta främst för att främja konkurrens och innovationskraft.

Den tekniska basen för OCIT: s gränssnitt är Internetteknologi, därför möjliggörs trafikmanagementsystem och vidsträcka nätverk som omfattar centraler och fältstationer.

11.3.2 Medverkande i OCIT

OCIT består av tyska grupperingar med skilda intressen och uppgifter men med det gemensamma att de alla är verksamma inom området vägtrafikteknik. De är organiserade i form av ett ”runt bord” där att alla har lika mycket att säga till om. Det runda bordets viktigaste funktion är att likställa krav och önskemål från städer och planeringsbyråer jämtemot den ekonomiska press som finns från leverantörers och kunders sida. Verksamma i OCIT är Open Traffic Systems City Association e.V (OCA), Verband ders Ing. Büros für Verkehrstechnik (VIV), OCIT Developer Group (ODG) och Open Communcation for Traffic Engineering Components (OTEC).

OCA är en sammanslutning av tyska städer vars främsta intresse är att säkerställa de krav på funktionssäkring och harmonisering som finns på OCIT: s gränssnitt samt att påverka industrins utvecklingsarbete.

VIV är en sammanslutning av tyska ingenjörsbyråer som arbetar med trafikteknik. Deras uppgift i OCIT är att arbeta med de rekommendationer som OCA har angående framtagning av OCIT-system och komponenter.

ODG är arbetsgemenskap av tyska företag som arbetar med trafikstyrningssystem och dess komponenter. Deras uppgift i OCIT är att åskådliggöra tekniska lösningsvägar och omsätta resultaten i tekniska specifikationer för sina system och komponenter.

OTEC är ett konsortium av företag för standardisering av kommunikation mellan komponenter i vägtrafikteknik. Deras uppgift i OCIT är att åskådliggöra tekniska lösningsvägar och omsätta resultaten i tekniska specifikationer för sina komponenter.

11.3.3 Protokoll i OCIT

OCIT är uppdelat i olika gränssnittsområden, de två som berör protokoll är Instations och Outstations. Där Instations gränssnitt är mellan centrala komponenter och system och Outstations gränssnitt är mellan central och fältapparater.

Instations

För Instations pågår arbetet med att fastställa gränssnitten, fastställt idagsläget är att gränssnitten kan ses som dataflöden mellan komponenter och system. Kraven på protokollet skiljer sig åt beroende på om tjänsten är automatisk eller manuell, datamängd och -sort. Vad man kommit fram till hittills är följande:

- Dataöverföringen ska orientera sig efter OSI-modellen
- Användning av XML för databeskrivningen
- Dataöverföringen ska kunna använda alla sedvanliga medier och telekommunikationstjänster. I första hand Ethernet LAN och WAN.

Outstations

För Outstations finns en kommunikationsmodell med protokoll fastställd, den beskrivs nedan.

11.3.4 Kommunikationsmodell

Dataöverföringen orienterar sig efter OSI-modellen. I skikt fem till sju används det egenutvecklade OCIT-Outstation protokollet Basis Transport Paket Protokoll Layer (BTPPL) som beskrivs nedan. I skikt fyra används standardprotokollen TCP och/eller UDP. Normalt stöder fältapparater både TCP och UDP, men vissa resursfattiga apparater stödjer enbart UDP. I skikt tre används standard IP och skikt ett och två är ej standardiserade.

OSI-skikt	OCIT: s protokoll
7	BTPPL
6	
5	
4	TCP UDP
3	IP
2	Fritt valbart, ex PPP
1	Fritt valbart

Tabell 3 Sammanställning av protokoll använda av OCIT

11.3.5 Användning

I dagsläget används OCIT i två testområden i de tyska storstäderna Frankfurt och Dortmund, där testas kommunikation med hjälp av OCIT-Outstations gränssnitt. Annars är som tidigare nämnts OCIT: s arkitektur fokuserad på ITS och förbered för användning inom en mängd olika områden (exempelvis information, parkering, landsort). Typiska uppgifter är betjäning

och övervakning av apparatfunktioner på distans, varvid ögonblickliga kvitteringar, reaktioner och felbehandlingar sker.

11.3.6 Tillgänglighet

För att få använda sig av OCIT krävs medlemskap i OCIT, kostnaden för medlemskap är ej känd.

11.4 Technische Lieferbedingungen für Streckenstationen (TLS)

Technische Lieferbedingungen für Streckenstationen (TLS) är en tysk standard med målet att enhetligt fastställa funktioner och gränssnitt för apparater som används för att samla in och behandla trafikinformation. Detta görs för att apparater från olika leverantörer ska ha till stor del samma prestationsförmåga och därmed enkelt ska gå att jämföras. För tillverkarna av apparater ska TLS tjäna som avgränsning av vilka egenskaper deras apparater ska ha och möjliggöra fri konkurrens.

11.4.1 Omfattning

I TLS definieras funktionella krav och gränssnitt för apparater som styr variabla skyltar, samlar in trafikdata, och samlar in omgivningsdata. Information inrapporterad från bland annat polis, vägbyggnations- och trafikmyndigheter till kartläggningssystem ska kunna tas tillvara och påverka styrningen av variabla skyltar. Utformningen av vägstationer med avseende på energiförsörjning, klimatförhållanden, överspänningsskydd, etcetera är definierat.

TLS är till stor del anpassat och framtaget för kommunikation och informationshantering kring det tyska motorvägsnätet. Mer om detta nedan, under Systembeskrivning.

11.4.2 Medverkande

TLS är framtaget av den statliga tyska förvaltningen Bundesanstalt für Straßenwesen (BASt) i samarbete med industrin och delstatsförvaltningen (Länderverwaltung).

11.4.3 Systembeskrivning

Nedan ges en kortfattad beskrivning av det system som TLS är anpassat för.

Systemnivåer

På grund av den rumsliga utbredningen av det tyska motorvägsnätet och andra omständigheter så är nätverket uppdelat i flera enskilda regionala nätverk. För att kunna behärska den

förväntade datauppkomsten är varje regionalt nätverk uppdelat i flera hierarkiska nivåer, se tabell 4 för de olika nivåerna och dess roll.

Nivå	*Inrättning*	*Plats*
1	*Trafikräkningscentral*	*Central punkt i motorvägsnätet i en region*
2	*Undercentral, tjänar exempelvis till styrning av variabla skyltar*	*Exempelvis i motorvägsmästeriet eller i trafikräkningscentralen*
3	*Styrmodul och överföringssystem i den lokala stationen*	*Vägstation*
4	*Dataregistrerings- och datautgivningsapparater med I/O-koncentratorer för lokal data aggregering, för utvärdering av data, respektive för överlämnande av parametrar och ställkommandon*	*Vägstation*

Tabell 4 Hierarkiska nivåer i TLS (Källa: TLS utgåva 2002)

Trafikräkningscentralen kommunicerar med undercentralen över fjärrbussen, undercentralen kommunicerar med stationens styrmodul över öbussen och styrmodulen kommunicerar med de olika dataregistrerings- och datautgivningsapparaterna över lokalbussen.

Styrmodulen och dataregistrerings- och datautgivningsapparater i nivå 3 och 4 ryms i regel i ett och samma vägskåp.

Funktionsfördelning

Varje av de ovan nämnda nivåerna har speciella funktioner att uppfylla. Funktionerna ska avstämmas efter varandra och fördelas så att överföringsbehovet inte överstiger överföringskapaciteten. Endast data som behövs i nästa nivå ska vidarebefordras dit.

Nivå 1 och 2 funktioner beskrivs ej i denna rapport, då de har ringa relevans. De finns beskrivna i Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen.

Nivå 3 och 4 huvudfunktioner är följande:

Styrmodul:

- Styrning av datautbytet mellan undercentral och I/O-koncentrator
- Styrning av begäransrytm och överföringsproceduren för I/O-koncentratorerna på lokalbussen

I/O-koncentrator:

- Registrering och aggregering av trafik- och omvärldsdata från anslutna sensorer
- Vidarebefordra styrkommandon till variabla skyltar
- Funktionsövervakning och statusmeddelanden

Överföringsnät

För dataöverföringen mellan vägstation och undercentral finns i regel ett kabelpar (BAB-Streckenfernmeldekabels) till förfogande, där data kan skickas i halvduplex med hastigheten 1200 Bit/s. Dataöverföringen inom vägstationen sker med hjälp av en buss förbindning som består av två tvinnade ledningar som följer standarden RS485.

11.4.4 Kommunikationsmodell

TLS kommunikationsmodell orienterar sig efter OSI-modellen. I TLS används ett eget protokoll som motsvarar skikt 2, 3 och 7. Skikt 4-6 egenskaper saknar motsvarande egenskaper i TLS. Skikt 2, 3 och 7 beskrivs var för sig nedan.

OSI-skikt	TLS
7	TLS skikt 7
6	Inget
5	
4	
3	TLS skikt 3
2	TLS skikt 2
1	Valbart

Tabell 5 Sammanställning av protokoll i TLS

11.4.5 Användning

TLS används kring det tyska motorvägsnätet.

11.4.6 Tillgänglighet

TLS tillgänglighet är oklar, sannolikt är det en förhandlingsfråga med den tyska förvaltningen.

12 Vad bör göras?

Som beskrivits tidigare finns en problembild med användandet av olika protokoll och definitioner av datainnehåll, främst i och med avsaknaden av utbytbarhet av apparater och interoperabilitet. Enda relevanta sättet att upphäva dessa problem är en standardisering av både protokoll och datainnehåll. Nedan granskas om en standardisering bör ske.

12.1 Varför standardisera?

Normalt avgörs vilket (vilka) protokoll som används till ett projekt av det enskilda projektet och vilka (vilken) leverantör som är involverade i det. Ett resultat av detta är att en utvidgning av ett system generellt sett endast kan ske om nya apparater är från samma leverantör som initialt har levererat till det aktuella systemet. Andra apparattyper och apparater från andra leverantörer kan implementeras om stora investeringar görs för systemintegration.

Detta leder till att det är liten till obefintlig chans för realistiskt konkurrenskraftiga upphandlingar av ytterligare apparater vid utökningar av ett system, på grund av avsaknad av utbytbarhet. Möjligheten till att ansluta ytterligare apparattyper till systemet minskar betydligt, på grund av avsaknaden av interoperabilitet.

Den begränsade chansen till realistiskt konkurrenskraftiga upphandlingar gör att det är en uppenbar risk för att ett företag eller en liten grupp av företag får en monopolställning på marknaden. Detta har skett i Sverige inom området trafiksignaler, där Peek Traffic har levererat sitt system till ett stort antal städer. Enligt uppgifter från konkurrenter och Peek Traffic är det i princip omöjligt för andra att anpassa sig till protokollet Peek Traffic använder sig av till annat än för ren övervakning, då protokoller utgör en del av funktionaliteten i deras styrapparat.

Således är de största anledningarna till en standardisering av protokoll och datainnehåll möjligheterna till utbytbarhet av apparater och interoperabilitet, och de fördelar de medför. För- och nackdelar med en standardisering beskrivs nedan.

12.2 Nyttan med en standardisering?

Nyttan med en standardisering finns främst i möjligheterna till utbytbarhet av apparater och interoperabilitet. Utbytbarhet av apparater skulle medföra betydligt bättre konkurrensvillkor vid upphandlingar av ytterliggare apparater och vid utbyte av defekta apparater. Interoperabilitet skulle medföra möjligheter till gemensamma nätverk för olika typer av apparater och möjliggöra att framtida typer av apparater kan anslutas till befintliga nätverk.

De för- och nackdelar som finns med en standardisering beskrivs nedan. Att tänka på är att en del fördelar endast uppkommer vid en omfattande standardisering, detta kommenteras kontinuerligt.

12.2.1 Fördelar med en standardisering

Val av leverantör

Ett system som stödjer en standard kan kommunicera med vilken produkt som helst från andra leverantörer som stödjer samma standard. Detta leder till att antalet leverantörer, system, fältapparater och mjukvaror som kan övervägas vid köp ökar markant. Leverantörsspecifika finesser blir endast tillgängliga för mjukvaror och produkter från samma leverantör, basfunktionaliteten beskriven i standarden blir tillgänglig oavsett leverantör.

En standardisering gör det enklare att gradvis byta ut mjukvara, styrapparater och andra fältapparater från en leverantör till en annan, istället för att behöva byta ut hela systemet om man vill byta leverantör. Ytterligare en fördel är att problem med reservdelar minskar. Exempelvis kan avsaknad av reservdelar på grund av att en leverantör gått i konkurs lösas enkelt genom att den apparat som gått sönder byts ut mot en från en annan leverantör.

Fördelen att kunna välja leverantör beror på om både protokoll och datainnehåll standardiseras, mer om detta nedan i kapitel 13.2 ”Vad bör standardiseras ur en teknisk synvinkel?”. Självklart är det enbart de ITS-områden som standardiseras som berörs av denna fördel. Sammanfattningsvis leder det friare valet av leverantör till att möjligheterna för frikonkurrens ökar avsevärt och således finns goda möjligheter till bättre pris- och kvalitetskonkurrens.

Koordination mellan väghållare

Standardisering möjliggör att väghållare kan utbyta information och med hjälp av enkla kommandon (och auktorisering) följa förhållandena i andra väghållares system. Vilket gör att koordinerade gensvar kan implementeras vid olyckor och andra förändringar i fältförhållandena. En väghållare kan övervaka och iscensätta baskommandon (om auktoriserad) till fältapparater styrda av en annan väghållare.

Exempel på applikationer med potential för koordination mellan väghållare är:

- Koordinerade trafiksignaler över juridiska gränser, för svensk del vid gränsövergångar
- Tillhandahålla trafiksignalprioritering för utvalda (ex. försenade bussar)
- Tillhandahåll realtidsinformation till en gemensam resandeinformationscentral
- Övervaka trafikvolymer på en annan väghållares vägnät
- Lägga ut ett varningsmeddelande på en annan väghållares variabla skylt

Flertalet av dessa fördelar kräver att standardiseringen omfattar kommunikation mellan centraler, vilket sannolikt inte är aktuellt i första skedet av en standardisering. Det som kan vara av intresse är om användningen av informationsutbyte mellan olika ITS-områden förenklas, vilket borde vara möjligt om kommunikationen är standardiserad, då information kan ”avlyssnas” av andra områden än vad den primärt är avsedd för.

Användande av ett kommunikationsnätverk

En standardisering kan medföra att ett ledningssystem kan kommunicera med en blandning av apparattyper på samma kommunikationskanal. Kommunikationsnätverket är vanligtvis en av de dyraste komponenterna i ett transportledningssystem, således finns ekonomiska fördelar.

Denna fördel förutsätter att det är mer än ett ITS-område som standardiseras. Till viss del kan fördelen även göra så att andra nät kan utnyttjas genom att standarden stödjer användande av TCP/IP, då detta gör att vanliga telekommunikationsnät går att använda i stor utsträckning.

Bättre utdata

I dagsläget utnyttjas inte den utdata som genereras från många ITS-system, då data från dessa aggregerats efter systemens enskilda behov eller försummas på annat sätt. Detta gör att kostsamma separata datainsamlingar måste göras eller att mer eller mindre grova uppskattningar används för att tillgodose de behov av data som behövs för prognoser och forskning. En standardisering kan medföra att utdata tillgängliggörs till lägre kostnad, bättre säkerhet samt med bättre kvalité.

Denna fördel kräver att icke aggregerad data lagras centralt, varifrån den sedan kan hämtas och bearbetas.

Forskning

För forskning kan en standardisering ha betydelse på flera sätt. Dels kan bättre utdata ha betydelse för forskning som är beroende av bra prognosunderlag och/eller bra historiska data. Exempel på sådan forskning är forskning inom olycksutveckling och trafikutveckling. Dels kan standardiserade för styrning av apparater tillsammans med bra prognosunderlag leda till bättre möjligheter för forskning inom avancerade övervaknings- och styrsystem.

Kontaktade personer med erfarenhet från forskning ser endast begränsade fördelar med en standardisering ur denna synvinkel.

Övriga fördelar

Kommunikationen är designad för ITS och efter dess önskemål.

12.2.2 Nackdelar med en standardisering

- Merkostnader för leverantörer som måste anpassa sina apparater efter standarden
- Kostnader för anpassning av gamla apparater
- Gamla utrustningar som inte går att anpassa till aktuell standard på grund av bland annat för låg processorkapacitet och liknande kan leda till merkostnader för att byta ut utrustningar i ett tidigare skede än planerat eller till drift av gamla system parallellt med ett nytt

- Kostnader och resursbehov för införande och anpassningar av en befintlig standard alternativt ta fram en ny standard
- Eventuellt mindre flexibelt än mer specifika lösningar

Kostnadernas storlek varierar beroende på hur omfattande standardiseringen är och vilka ITS-områden som berörs.

12.3 När bör en standardisering ske?

Vid en standardisering är det viktigt att tidpunkten är den rätta. Enligt Donald A. Norman (The Design of Everyday Things) ska en standardisering inte ske för tidigt, då detta kan leda till att man låser sig till en primitiv lösning eller inför regler som visar sig vara mycket ineffektiva eller fel framkallande. Norman hävdar även att om det standardiseras för sent så kan det redan finns så många lösningar så att de involverade inte kan komma överens om en standard, speciellt om användningen av de olika lösningarna är utbredd.

För ITS-området gäller att en världsomfattande internationell standardisering är mycket svår att genomföra. Mestadels på grund av skilda synsätt och normer, men även delvis på grund av att olika mer eller mindre internationella standarder redan finns (exempelvis NTCIP i USA) eller är under utveckling. Vad gäller tidpunkten så skiljer det sig något åt beroende på vilken del av ITS-området man betraktar. Klart är att det inte är för tidigt med en standardisering inom de områden som finns i bruk i någorlunda omfattning, faktum är att det snarare är tvärtom för vissa delområden.

För området trafiksignaler skulle det vara önskevärt att en standardisering genomförts för flera år sedan. Det kommer antingen blir ekonomiskt betungande att genomföra en standardisering för området trafiksignaler, då det finns många och skulle vara dyrt att modifiera alternativt byta ut de apparater som används eller så skulle befintliga system behöva vara i drift parallellt under lång tid. För området variabla skyltar är tidpunkten bättre då det finns färre och de allmänt sett är modernare, vilket medför att det finns större möjligheter till modifiering av dem till en gynnsam kostnad.

12.4 Slutsatser

En standardisering är att rekommendera om kostnaderna för en sådan anses rimliga och resurserna finns tillgängliga, då fördelarna med utbytbarhet av apparater och interoperabilitet är stora samt att de enda relevanta nackdelarna med en standardisering är ekonomiska. Långsiktigt kan det vara ekonomiskt med en standardisering då det ger samordningsvinster, speciellt i användandet av nätverk, samt ökar konkurrensen, vilket ger utsikter om bättre pris och kvalitet.

För att utröna detta är en ekonomisk analys önskvärd, som ger svar på långsiktig ekonomisk påverkan samt ett kostnads/nyttoförhållande. En standardisering bör ske även om kostnaderna är höga, då man med en standardisering undviker monopolbildningar, leverantörsberoenden samt får en bättre konkurrenssituation. Möjligheter finns till att en standardisering kan ha viss betydelse för forskning med behov för bra prognosunderlag och/eller historiska data samt för forskning inom avancerade övervaknings- och styrsystem.

Tidpunkten för en eventuell standardisering är förhållandevis lämplig. Förmodligen hade det varit bra om en standardisering redan utförts, speciellt för området trafiksignaler. Sammanfattningsvis för tidpunkten kan sägas att det är något slags nu eller aldrig läge, där slutsatsen som kan dras är att en standardisering bör ske snarast möjligt eller inte alls.

Fortsättningsvis i denna rapport förutsätts att kostnaderna är rimliga och att resurser i form av ”know-who” finns tillgängliga så att en standardisering kan ske. Ett resonemang kring hur kostnader kan komma att påverka en standardisering är viktigt, då detta är det främsta argumentet mot och största hindret för en standardisering. Fortsatt frågeställning blir ”Hur bör det göras?”.

13 Hur bör det göras?

Klarlagt är att en standardisering bör ske vid rimliga kostnader och förutsatt att resurser i form av ”know-who” finns tillgängligt, detta håller merparten av de personer med branschkännedom som kontaktas under arbetet med om. Frågeställningen här är hur en standardisering bör göras. Denna frågeställning kan delas upp i följande delfrågor:

1. Vilka ITS-områden bör omfattas av standardiseringen?
2. Vad bör standardiseras ur en teknisk synvinkel?
3. Vilka aktörer och länder bör vara engagerade vid en standardisering?
4. Bör en ny standard utvecklas eller bör en befintlig internationell standard implementeras?

Respektive fråga diskuteras nedan och rekommendationer ges, avslutningsvis sammanfattas rekommendationerna i kapitel 16, ”Resultat”. Den kommunikation som i första hand anses befogade att standardisera är den mellan central och apparat samt den mellan apparater.

13.1 Vilka ITS-områden bör omfattas av en standardisering?

Inom ITS finns ett antal områden som har eller kan ha nytta av standardiserad kommunikation från central till apparat respektive apparat till apparat. De områden som i dagsläget främst kan tänkas ha nytta av en standardisering är kommunikation till/från/mellan trafiksignaler, variabla skyltar och VViS stationer. Dessa olika områden skulle vid användande av samma protokoll kunna använda sig av samma nätverk i större utsträckning än vad fallet är idag, samt lättare kunna tillgodogöra sig information från de andra systemen/områdena.

Givetvis är det fördelaktigt om andra områden stöds fast de i dagsläget inte har någon spridning eller endast används på ett fåtal platser. Potentiellt sett kan detta leda till ekonomiska fördelar och förenkla införandet av nya system, då ett befintligt eller delar av ett befintligt nätverk enkelt kan användas. Exempelvis kan ett befintligt nätverk för kommunikation till variabla skyltar och trafiksignaler användas vid införandet av ett nytt parkeringssystem. Detta gör att det eventuellt endast behövs byggas korta sträckor av anslutningar till det befintliga nätverket, vid själva parkeringshuset och vid skyltar. Detta gör att nyttopotentialen ökar.

Optimalt är alltså att så många områden som möjligt standardiseras då det finns möjligheter till ekonomiska vinster samt möjligheter till förenkling av användandet av andra systems/områdens data. Rekommendationen här är således att en standardisering om möjligt sker med en gemensam standard för så många områden som möjligt, då detta kan anses optimalt ur nyttosynvinkel. Viktigt är att området trafiksignaler omfattas, men även området variabla skyltar bör omfattas, då dessa två områden har störst utbredning. Övriga områden är önskvärda men ej lika viktiga. Utrymme bör givetvis finnas för att framtida områden ska kunna använda samma protokoll. Realistiskt är att börja med att standardisera kommunikation för områdena trafiksignaler och variabla skyltar för att beroende på behov, vilja och ekonomiska förutsättningar standardisera övriga områden.

Problem finns främst inom området trafiksignaler, som har störst utbredning, där många i branschen anser det för dyrt att standardisera. Ett utvärderingsarbete/förstudie pågår på nordisknivå över detta område. Denna utvärdering/förstudie görs av en dansk konsult som fått uppdraget av NEXT, som är en gemensam arbetsgrupp av signaltekniker från nordiska väghållare.

13.2 Vad bör standardiseras ur en teknisk synvinkel?

Vid en standardisering finns det några viktiga tekniska aspekter att ta hänsyn till. För att en av de största fördelarna med en standardisering, utbytbarhet av apparater, ska realiseras måste datainnehållet i protokollet vara standardiserat. Det är detta som möjliggör att olika fabrikat av apparater kan förstå varandra och att apparater kan bytas ut mot en apparat av samma typ men från annan leverantör. Även för att delar av den andra stora fördelen med en standardisering, interoperabilitet, ska realiseras måste datainnehållet vara standardiserat. Utan standardisering av datainnehållet kan inte apparater från olika leverantör förstå varandra och de kan således inte arbeta tillsammans på samma sätt i ett system som de skulle kunna om de förstod varandra.

Datainnehållet kan antingen standardiserats helt eller så kan en basfunktionalitet standardiseras och möjligheter ges för leverantörsspecifika funktioner. Bägge två av dessa varianter har sina för- respektive nackdelar. Fördelar med en hel standardisering är att ingen leverantör kan skaffa sig ett bättre konkurrensläge än sina konkurrenter vid utbyggnationer av system de levererat, där delar av systemets applikationer bygger på leverantörsspecifika funktioner. Nackdelar med en hel standardisering är att det begränsar innovations- och prestationsförmåga hos de olika leverantörerna, vilket försämrar konkurrenssituationen. För en standardisering med basfunktionalitet och möjligheter för leverantörsspecifika funktioner är för- respektive nackdelarna de omvända. Det bästa här är att standardisera basfunktionaliteten noggrant och omfattande, då kan leverantörsspecifika funktioner tillåtas utan att de leder till beroende av leverantörsspecifika funktioner. Lämpligt är att efterhand lägga till de leverantörsspecifika funktionerna som bedöms öka standardens kvalité. Viktigt är att datainnehållet går att komplettera för kommande behov, vilket merparten av de tillfrågade i branschen håller med om.

En standardisering av datainnehållet finns det personer i branschen som delvis reserverar sig mot då de anser att med största sannolikhet leder till dyrare apparater, som inte uppväger nyttan det ger. De tycker även nyttan är begränsad, men det beror förmodligen på att de inte ser till hela processen, samt till möjligheterna till bättre konkurrens som uppstår.

För att resterande fördelar med interoperabilitet ska finnas krävs en standardisering av de/det protokoll som bär data mellan centraler och fältapparater. Detta möjliggör att samma överföringsmedium/nätverk kan samutnyttjas. För bärprotokollen är det viktigt att TCP/UDP och IP stöds, detta innebär att det finns möjlighet att välja alla på marknaden tillgängliga medier (fiber, koaxkablar, kopparkablar, GPRS, WLAN, Radio-LAN) för anslutning av apparater samt att det möjliggör användande av telefoninätet. Fördelaktigt är även om många standardprotokoll används, då detta ger bra möjligheter till användande av standardprodukter.

Det är även viktigt att inte låsa sig kring någon speciell lösning i skikt 1 och 2 i OSI-modellen, då detta kan leda till problem i och med de vitt skilda placeringarna av

fältapparater. För decentralt placerade apparaterna som antingen förbinds via en telefonledning eller med hjälp av någon trådlös metod går det inte att kräva exempelvis att Ethernet ska användas i skikt 2.

Ett fåtal personer i branschen tycker att det räcker med en standardisering av bärprotokollen och en satsning på infrastrukturen kring vägnätet, då detta ger möjligheter till gemensamma nätverk samtidigt som de tror att det inte medför dyrare apparater i samma utsträckning som en standardisering av datainnehållet.

Andra saker som är viktigt att tänka på är att utdata från apparater är lika viktigt som indata till dem. För utdata är det fördelaktigt om data inte förloras genom aggregering eller på annat sätt. Krav på låg processorkraft och bandbredd är också positivt då detta ökar chansen till att gamla apparater går att uppdatera så att de följer standarden. Givetvis är det även betydelsefullt om de mest frekventa befintliga systemen enkelt kan stödjas under en övergångsperiod, detta går förmodligen att göra genom protokollomvandlare. Fördelaktigt är även om någon sorts säkerhetsåtgärder finns vidtagna.

Rekommendation här är att både datainnehåll och bärprotokoll standardiseras för att uppnå samtliga fördelar, då det om endast en av dessa två standardiseras blir lite halvgjort och då kan man fråga sig om det inte är bättre att låta bli att göra något överhuvudtaget. Bättre genomföra en ordentlig lösning för att lösa de problem som finns idag än att göra något till hälften där flera problem kvarstår. Datainnehållet ska kunna kompletteras för kommande behov, samt att det är en fördel om det stödjer leverantörsspecifika funktioner. Viktigt är även att TCP/UDP och IP stöds då detta medför en mängd möjligheter med avseende på utnyttjande av befintliga nätverk. I OSI-modellens skikt 1 och 2 är det viktigt att flera olika lösningar kan användas. Fördelaktigt är även om många standardprotokoll används, säkerhetsåtgärder finns vidtagna samt att utdata inte gör förlorat.

13.3 Vilka aktörer och länder bör vara engagerade vid en standardisering?

För att en standardisering ska få genomslagskraft och företag ska lägga kraft och resurser på att ta fram välanpassade produkter som följer standarden krävs att en marknad finns för att produkter som följer standarden. Utan en tillräckligt stor marknad som efterfrågor produkter som stödjer standarden finns det stor risk att leverantörer gör dåliga lösningar för att anpassa sig till standarden så att de kan vara med och ge anbud, men att lösningen är bristfällig och leder till fördyrningar av produkten både på kort- och långsikt. Vissa företag kan även välja att inte anpassa sig efter standarden och istället koncentrera sig på andra produkter och marknader, då de anser att marknaden är för liten för att de ska vara värt att ödsla resurser på den.

Viktigt är alltså att incitament finns för de inblandande parterna. För beställare (exempelvis Vägverket och kommuner) finns detta i och med den ökade konkurrens mellan leverantörerna en standardisering medför. För leverantörerna kan lämpligt incitamentet vara en större marknad. Den svenska marknaden som helhet kan anses vara i minsta laget för att en generera nått större incitament från verksamma leverantörer, förmodligen skulle ett visst intresse finnas men det skulle ge bättre genomslagskraft om Sverige gjorde en standardisering tillsammans med fler länder. Eventuellt kan ett användande av en internationellt etablerad standard göra så

att intresset ökar ytterligare, då företagen då har andra marknader att saluföra sina produkter hos. Samtidigt finns det vissa problem här då inga internationella standarder kan implementeras rakt av p.g.a. skilda synsätt och normer. Lämpligt är att försöka få med övriga nordiska länder i en standardisering, då dessa har liknande synsätt och normer.

I vilken utsträckning branschföretagen bör medverka i en standardisering kan ses som en fråga om hur organisationen ska se ut som ska genomföra standardiseringen. Denna fråga är svår att svara på och beror till stor del på vilken typ av standardisering som ska genomföras. Detta gäller även andra branschaktörer som vägverk och kommuner. Lämpligtvis fastställs vilka branschaktörer som ska medverka med standardiseringsarbetet under en studie för hur ett införande av en standard ska gå till.

Rekommendation är att försöka få med övriga nordiska länder i ett standardiseringsarbete för att öka genomslagskraften. Att ett genomförande av en standardisering bör ske med just övriga nordiska länder beror på att de har liknande signaltekniska traditioner och en fungerande samsyn, vilket medför att en gemensam standardisering lättare kan genomföras. Vilka branschaktörer som ska medverka med standardiseringsarbetet bör fastställs i ett senare skede.

13.4 Bör en ny standard utvecklas eller bör en befintlig internationell standard implementeras?

Det finns tre alternativ för införandet av en standard.

1. Skapa en helt ny standard
2. Använda en befintlig standard som bas för utvecklande av en ny ITS-standard
3. Implementera och konvertera en internationell standard med ITS-anknytning

Att skapa en ny standard kan uteslutas direkt, då det skulle bli väldigt dyrt jämfört med att använda sig av en befintlig standard eller vidareutveckla en befintlig standard.

Spontant kommer tanken att användandet av en industristandard är ett sämre alternativ än att använda en standard utvecklad för ITS-området. På grund av att en standard från produktionsindustrin ej är anpassad för ITS på samma sätt som en ITS-standard och för att det kan antas att de kräver mer anpassningsarbete för att kunna implementera dem.

Detta resonemang är delvis rätt, då standarderna från produktionsindustrin är framtagna med till viss del andra problembilder. Resonemanget är även delvis fel då det finns många företag som tar fram olika typer av komponenter i förhållandevis stora volymer som stödjer dessa standarder, vilket gör att det generellt sett borde ge en bättre prisbild.

Standarder från produktionsindustrin kan vara omöjliga att implementera som en standard för hela dataflödet från central till fält, på grund av att de är framtagna efter en problembild som är vitt skild ITS-områdets problembild, vilket leder till att vissa erfordrade funktioner saknas. I de fall standarderna från produktionsindustrin inkluderar en standardisering av datainnehållet måste den till stor del omdefinieras. Detta gäller även till viss del standarderna med ITS-anknytning, då det finns nationella synsätt och normer för styrning inom de olika områdena. De största skillnaderna finns i området trafiksignaler. För övriga ITS-områden är det inte lika stora skillnader.

Sammanfattningsvis kan sägas att det med största sannolikhet medför ekonomiska fördelar i och med det mindre behovet av anpassning att använda sig av en ITS-standard, vilket även framgår av de frågor som ställts till personer i branschen. Samtliga tillfrågade är av åsikten att befintliga standarder ska användas i så stor utsträckning som möjligt.

Rekommendation är att utvärdera de internationella standarder från produktionsindustrin och de med ITS-anknytning som tidigare beskrivits med bakgrund av de rekommendationer som gjorts i tidigare avsnitt. Fokus i utvärderingen bör ligga på de standarderna med ITS-anknytning, då dess potential kan anses större, på grund av att de är utvecklade för ITS. Om ingen av dessa standarder anses överensstämma med de rekommendationer som gjorts bör den standard som överensstämmer mest användas som bas för utvecklandet av en ny standard. Förmodligen blir ingen standard från produktionsindustrin aktuell att använda för en standardisering i annat fall än om någon standard ska användas som bas vid nyutveckling.

14 Utvärdering av protokoll och standarder

Nedan kommer de internationella standarder från produktionsindustrin och de med ITS-anknytning som tidigare beskrivits betraktas med bakgrund av de rekommendationer som givits i tidigare kapitel, främst de tekniska rekommendationerna. De icke standardiserade protokollen kommenteras i viss mån, men hänsyn till deras möjligheter vid en standardisering.

14.1 Icke standardiserade protokoll använda i Sverige

Information om dessa protokoll är inte fritt tillgänglig, delvis på grund av affärssekretess skäl och förmodligen även i vissa fall på grund av saknad alternativt dålig dokumentation. Ett företag (Stunt AB) vill inte lämna ut någon information om sitt protokoll överhuvudtaget, övriga företag har alla bidragit med viss information om sina protokoll alternativt hänvisat till de standarder de använder sig av.

Enda protokollet/standarden som på något sätt skulle kunna användas vid en standardisering här är STCIP, Peek Traffics derivat på den amerikanska standarden NTCIP. För övriga protokoll gäller endast att det är fördelaktigt om de kan stödjas under en övergångsperiod.

STICP skulle eventuellt kunna användas vid en standardisering om det beslutas att en sådan ska genomföras och NTCIP ska användas. Ett användande av STCIP ger sannolikt en tidsvinst, men ingen kostnadsbesparing då någon måste stå för dess utvecklingskostnader. Stora problem finns även i och med att Peek Traffic är en stor marknadsaktör och får stora fördelar vid ett beslut av att använda STCIP. Det är även oklart i hur stor mån STCIP är förändrat från NTCIP. Detta är saker som får diskuteras om det beslutas att en standardisering ska genomföras och att den ska ske genom användande av NTCIP.

14.2 Relevanta världsstandarder från produktionsindustrin

I denna rapport har tre standarder från produktionsindustrin beskrivits, fler finns som har liknande möjligheter till användning inom ITS-området. Allmänt för standarder från produktionsindustrin är att de är utbredda och använda i många olika sammanhang, av många olika företag. Nedan följer kommentarer om respektive standard.

Generellt kan sägas att skulle bli svårt att få produkter certifierade hos de organisationer som står bakom standarderna från produktionsindustrin då alltför stora förändringar skulle krävs innan en sådan kan används som standard för ITS-kommunikation. Det en standard från produktionsindustrin kan användas till är att den kan utgöra grund för utvecklandet av en ny ITS-standard och en del av produkter framtagna efter denna standard kan användas. Eventuellt kan en ITS profil skapas i standarden.

Oavsett standard krävs stora omarbetningar eller tillägg till befintliga definitioner av datainnehållet för att det ska passa till användande inom ITS-området.

14.2.1 CanOpen

CanOpen är inte aktuellt att använda vid en standardisering av kommunikationsflödet från central till fältapparat, detta då CanOpen inte alls är utvecklat för användande i stora nätverk. CanOpen är främst anpassat för inneslutna nätverk (främst CAN) som finns i bland annat olika typer av fordon. Vilket märks då det inte använder sig av TCP/UDP och IP, vilket är en av rekommendationerna vid en eventuell standardisering.

Det bygger även på en funktion, normalt tillhandahållen av det underliggande CAN-protokollet, som främst är lämpad för en mindre nätverk. Funktionen i fråga är användandet av Broadcast meddelanden vilken inte är lämpad för användare-till-användare kommunikation.

14.2.2 Modbus

Modbus stödjer både kommunikation med token, seriell kommunikation och TCP/IP kommunikation. Dessa tre typer av kommunikation kan kombineras ihop genom gateways och hindrar således inte kommunikation mellan apparater anslutna via olika protokollstackar. Att flera typer av kommunikation kan användas är positivt, då det ger fler möjligheter och mera valfrihet vid en eventuell standardisering. Problem finns i och med att protokollen i skikt 2 och till viss del skikt 1 inte är fritt valbara.

Datainnehållet är även det standardiserat till stor del. Denna standardisering sker genom användande av funktionskoder. Där funktionskoden indikerar vilken sorts operation som skall utföras. Det finns olika typer av funktionskoder, den största delen av dem är fördefinierade genom organisationen bakom Modbus. Förmodligen skulle det krävas en hel del arbete här för att anpassa till ITS-applikationers behov.

14.2.3 Profibus

Profibus tillsammans med PROFInet skulle principiellt kunna användas vid en standardisering, där Profibus används för kommunikationen mellan fältenheter och PROFInet för kommunikationen mellan PLC:er, industriPC och IT-system i kontorsvärlden. Problem är att det Profibus inte stödjer TCP/UDP och IP, vilket gör att PROFInet måste användas i storutsträckning. I PROFInet används Ethernet i skikt 2 vilket inte är lämpligt vid en standardisering, då det är orealistiskt att ha detta vid alla apparatplaceringar.

I PROFInet är skikt 5, 6 och 7 fritt valbara, detta ställer till vissa problem då två apparater som använder sig av olika protokoll i dessa skikt inte kan kommunicera direkt med varandra. Detta problem går att lösa med hjälp av gateway. Användandet av gateway medför extra kostnader och ställer till vissa problem vid eventuella utbytanden av apparater.

Datainnehållet är standardiserat i Profibus, detta åstadkoms genom att olika profiler används. För att full interoperabilitet ska uppnås i ett nätverk måste samma profiler användas. Vid en eventuell standardisering måste profiler anpassade för ITS tas fram. Eventuellt kan vissa delar tas från befintliga profiler samt från de datadefinitioner som används i MTM-systemet (använder sig delvis av Profibus) i Stockholm.

14.2.4 Slutsatser av utvärdering av standarder från produktionsindustrin

Att använda någon av de standarder från produktionsindustrin som finns med i denna rapport bör undvikas. Delvis på grund av att de inte är anpassade efter de förhållanden som råder inom ITS vad gäller avstånd och delvis på grund av det omfattande arbete som krävs för att datainnehållet ska vara enhetligt och anpassat efter ITS-applikationers behov. Problem finns med anpassning mot avsides belägna apparater bland annat genom de begränsade valmöjligheter som finns i OSI-modellens skikt 1 och 2.

Bland övriga standarder från produktionsindustrin kan det tänkas att det eventuellt finns någon standard som tillfredställer ITS-områdets behov med avseende på apparaternas skilda placeringar. Säkert är att det inte finns någon standard som definierar datainnehållet med avseende på ITS-applikationers behov. Dessa fakta leder till slutsatsen att det är fördelaktigt att använda sig av en befintlig standard som är utvecklad för ITS och dess behov, då detta med största sannolikhet ger ett minst lika bra resultat till ett lägre pris.

Det enda som skulle kunna tala för användandet av en standard från produktionsindustrin är möjligheterna till en bättre prisbild, då komponenter och produkter tas fram i förhållandevis stora volymer till dessa standarder. Förmodligen krävs så omfattande ändringar av standard från produktionsindustrin innan den kan införas vid en standardisering så att certifierade produkter från ursprungsstandarden endast kan användas i begränsad omfattning. Detta samt att merparten av standarderna med ITS-anknytning baseras på standardteknik gör att denna fördel är av ringa betydelse.

Slutsatsen som kan dras är att det bör undvikas att använda en standard från produktionsindustrin vid en standardisering, då dessa standarder är dåligt anpassad till de förhållanden som råder för ITS-applikationer samt för att arbetet med datainnehållet blir mer omfattande.

14.3 Världsstandarder med ITS-anknytning

I denna rapport har fyra standarder med ITS-anknytning beskrivits. De fyra standarderna skiljer sig markant åt vad gäller berörda ITS-områden och omfattning av standardisering. Nedan följer kommentarer om respektive standard med tyngdpunkt på tidigare rekommendationer.

För alla standarder gäller att det krävs en del arbete för att anpassa dem till svenska normer och synsätt. Detta gäller främst för området trafiksignaler som är funnits längst, vilket medfört att skilda nationella regelverk växt fram. Norden har en fungerande samsyn medan övriga Europa och världen skiljer sig markant åt. För övriga områden är detta inte lika stort problem då synsättet för dessa områden är förhållandevis lika mellan olika länder, till stor del beroende på internationella leverantörer och applikationernas ringa ålder.

Samtliga standarder stödjer användning av standardprotokoll eller använder sig till stor del av standardprotokoll från telekommunikationsindustrin, vilket är positivt. För utdata är det svårt att kontrollera hurvida data går förlorat, då detta kräver expertkunskaper samt fullständig tillgång till standardernas datadefinitioner. Av denna anledning tas det ingen hänsyn till detta, vilket har ringa betydelse då det har liten påverkan i valet av standard.

14.3.1 IVERA

IVERA är en enklare lösning för standardiserad kommunikation mellan främst trafiksignaler och en kontrollcentral. Det stödjer även kommunikation för påfartskontroll, kontroll av skyltar i parkeringssystem och sammanlänkar kontrollcentraler. Resterande områden som väderdetektorer och variabla skyltar stöds ej. Detta går förmodligen att lösa genom kompletterande standardiseringsarbete, vilket kräver resurser och tid.

I IVERA standardiseras både protokoll och datainnehåll. För protokoll standardiseras endast OSI-modellens skikt 7, men en rad antaganden görs med avseende på vad underliggande protokoll ska utföra. Inga av dessa antaganden är anmärkningsvärda. Viktigt att påpeka är att de möjliggör användande av TCP/IP. Problem är att fullständig interoperabilitet och utbytbarhet av apparater inte uppnås om inte samma protokoll används i skikten under skikt 7.

Datainnehållet i IVERA är standardiserat med en viss basfunktionalitet och möjligheter till tillverkarspecifika funktioner. Det stödjer införande av nya funktioner i standarden efter hand. För de områden som ej är standardiserade i IVERA krävs sannolikt kompletterande definitioner av datainnehållet för att basfunktionalitet ska uppnås, i vilken omfattning är oklart.

IVERA används i Holland och produkter anpassade efter standarden tillhandahålls av ett flertal branschaktörer.

Fördelar med IVERA är att det inte är lika omfattande som andra standarder, vilket sannolikt leder till positiva ekonomiska effekter för införandet. Övriga fördelar med IVERA är att det är framtaget med utgångspunkt att maximera användandet av standardkommunikationsinrättningar för både kommunikationsinfrastruktur och –mjukvara, vilket minimerar utvecklingsansträngningar och ger stöd till befintliga kommunikationsnätverk och protokoll. Positivt är även att det används.

Nackdelar med IVERA är att det inte stödjer flera av ITS-områderna samt de problem som finns med interoperabilitet och utbytbarhet av apparater i och med att endast skikt 7 är standardiserat. Förmodligen krävs att mycket arbete längs ner på kompletterande standardisering.

14.3.2 NTCIP

NTCIP är en komplett lösning för kommunikation mellan centraler och fältapparater samt för kommunikation mellan olika centraler. Alla tänkbara områden omfattas bortsett från kommunikation mellan styrapparat och annan elektronisk utrusning i ett RSC-skåp.

I NTCIP standardiseras både protokoll och datainnehåll. För protokollen finns vissa valmöjligheter i de övre skikten (motsvarande skikt 3-7 i OSI-modellen) för vilket protokoll som kan användas för en viss applikation. De lägsta skikten (motsvarande skikt 1-2 i OSI-modellen) är fritt valbara. Datainnehållet i NTCIP är definierat i detalj för respektive applikation. Möjligheter finns till leverantörsspecifika funktioner.

NTCIP används i dagsläget i USA och produkter anpassade efter standarden tillhandahålls av ett flertal branschaktörer. På den svenska marknaden har Peek Traffic utvecklat ett derivat av NTCIP som de kallar STCIP. STCIP omfattar center till apparat kommunikation.

Fördelar med NTCIP är främst att det omfattar i princip samtliga områden där det finns behov av standardisering, i stor utsträckning använder sig av standardprotokoll och att det används. NTCIP standardiserar även kommunikation mellan centraler samt en del ITS-applikationer som i dagsläget inte används i Sverige.

Nackdelar med NTCIP är att det fortfarande till viss del är under utveckling, har höga krav på processorkraft och minneskapacitet samt att det generellt sett kräver snabbare kommunikationer för samma mängd data.

14.3.3 OCIT

OCIT standardiserar kommunikation mellan centraler och fältapparater, främst för området trafiksignaler men det är även lämpat för andra områden som trafikdetektorer och variabla skyltar. I dagsläget pågår arbete med att standardisera kommunikationen mellan centrala system och komponenter. Sannolikt krävs en del kompletterande arbete för att OCIT ska kunna används för merparten av ITS-områdena, då det främst är utvecklat för trafiksignaler.

I OCIT standardiseras både protokoll och datainnehåll. Kommunikationen standardiseras från skikt 3 till skikt 7 i OSI-modellen. Skikt 1 och 2 är fritt valbara, i skikt 3 och 4:a används IP och TCP/UDP och i skikt 5,6 och 7 används det för OCIT framtagna protokollet BTPPL. Speciellt med BTPPL är att det har en liten header vilket medför kortare överföringstider, tar lite plats i minnet hos de apparater som stödjer standarden och har bra säkerhet.

Datainnehållet i OCIT är standardiserat med en viss basfunktionalitet och möjligheter till tillverkarspecifika funktioner. Det stödjer införande av nya funktioner i standarden efter hand. För de områden som ej är standardiserade i OCIT krävs sannolikt kompletterande definitioner av datainnehållet för att basfunktionalitet ska uppnås, i vilken omfattning är oklart.

OCIT är främst framtaget för de tysktalande länderna, målsättningen är emellertid att den ska få internationell utbredning. Flertalet av de största tyska trafiksignalföretagen stödjer utvecklingen av OCIT.

Fördelar med OCIT är att det stödjer utnyttjande av befintliga telekommunikationstjänster, vilket minskar kostnaderna. OCIT är nyutvecklat vilket medför att det är anpassat efter ny teknik och nya önskemål. Nackdelar med OCIT är att det fortfarande är under utveckling för vissa delar och att det endast är används i två testområden och då främst inom området trafiksignaler.

14.3.4 TLS

TLS fastställer funktioner och gränssnitt för apparater som används för att samla in och behandla trafikinformation, det vill säga variabla skyltar samt detektorer för insamling av väder och trafikmängder. Övriga ITS-områden omfattas ej. En komplettering av TLS så att

den omfattar även dessa områden kräver med största sannolikhet en mycket stor arbetsinsats, då TLS är anpassat efter andra förhållanden än de som råder i städer.

I TLS standardiseras protokoll och funktioner. Kommunikationen standardiseras i skikt 2, 3 och 7 i OSI-modellen. Skikt 1 är valbart med resterande skikt saknas. I skikt 2, 3 och 7 används ett egen utvecklade protokoll som kallas TLS skikt 2, TLS skikt 3 respektive TLS skikt 7. Mindre bra här är att TCP/UDP och IP således inte stöds.

Datainnehållet i TLS är inte standardiserat däremot finns funktioner standardiserade. Med detta menas att det finns definierat vilka funktioner som en apparattyp ska kunna utföra, men att hur data kodas och skickas mellan olika apparater inte är definierat. Detta gör att interoperabilitet i nätverket uppnås, men att utbytbarhet av apparater och interoperabilitet i systemet saknas.

TLS finns i drift kring det tyska motorvägsnätet.

Fördelar med TLS är att det används och att det förmodligen skulle gå att införa med ett begränsat behov av förändringsarbete, då de områden det ej omfattar har skilda normer och tillvägagångssätt mellan olika länder.

Nackdelar med TLS är främst att stöd för flera ITS-områden saknas och att datainnehållet inte är standardiserat, och de problem som det medför vad gäller interoperabilitet och utbytbarhet. TLS är även en förhållandevis gammal standard, vilket gör att den bland annat inte stödjer TCP/IP och är anpassat efter ett överföringsnät med lägre kapacitet än vad som idag finns på många ställen.

14.3.5 Standarder med ITS-anknytning jämförda med tidigare rekommendationer

För att avgöra vilken standard som passar bäst vid en standardisering undersöks, nedan, hur aktuella standarder med ITS-anknytning om det uppfyller de rekommendationer som ges i kapitel ”Hur bör det göras?”. Främst undersöks hur rekommendationerna uppfylls om vilka ITS-områden som bör omfattas av en standardisering och vad som bör standardiseras ur en teknisk synvinkel.

TLS är den av standarderna som i ringaste utsträckning uppfyller rekommendationerna. Omfattningen av TLS är begränsad till variabla skyltar och detektorer för insamling av väder och trafikmängder, således saknas bland annat området trafiksignaler. Ur teknisk synvinkel så saknas stöd för TCP/UDP och IP samt att datainnehållet inte finns definierat.

IVERA uppfyller rekommendationerna till viss del. Omfattningen är begränsad till trafiksignaler, påfartskontroll, kontroll av skyltar i parkeringssystem och sammanlänkning av kontrollcentraler, således saknas bland annat områdena variabla skyltar och väderdetektorer. Ur en teknisk synvinkel är det största problemet att endast skikt 7 är standardiserat, detta ger vissa problem med interoperabilitet och utbytbarhet av apparater.

OCIT uppfyller rekommendationerna till viss del. Omfattningen är främst inriktad mot trafiksignaler, fast en del andra områden stöds till viss del. Det är oklart i vilken omfattning

och hur bra lösningarna är för de andra områdena, då test endast utförts med trafiksignaler. Ur en teknisk synvinkel finns inget att önska.

NTCIP uppfyller i princip samtliga rekommendationer. Samtliga områden omfattas och ut en teknisk synvinkel finns inget att önska som inte uppfylls.

Av aktuella standarder med ITS-anknytning är det NTCIP som bäst uppfyller (den enda standard som uppfyller) de rekommendationer som tidigare givits i kapitel 13. Övriga standarder avviker i skild grad från rekommendationerna. Den standard som avviker minst från rekommendationerna bortsett från NTCIP är OCIT följt av IVERA och TLS.

14.3.6 Slutsatser av utvärdering av standarder med ITS-anknytning

NTCIP är den enda av granskade standarder som uppfyller de rekommendationer som tidigare givits. Detta gör att det är ett enkelt val att välja vilken standard som bör användas vid en standardisering. Det enda som skulle kunna tala emot ett användande av NTCIP vid en standardisering är de ekonomiska aspekterna. I vad som framkommit vid skrivandet av denna rapport så finns det inget som pekar på att NTCIP är dyrare att anpassa till svenska normer och synsätt samt att införa än någon annan standard, snarare tvärtom då ingen vidareutveckling av standarden krävs för att samtliga områden ska omfattas. Införskaffandet av produkter kan eventuellt vara något dyrare för NTCIP än för andra standarder, på grund av dess högre krav på processor- och minneskraft. Dessa ekonomiska aspekter bör utredas separat och leda till en ekonomisk rapport, lämpligtvis görs detta i samband med en kostnads- och nyttoanalys av en standardisering.

Speciella fördelar som finns med NTCIP är att NTCIP omfattar kommunikation för i princip alla tänkbara ITS-applikationer samt kommunikation mellan ledningscentraler och system. I ett första skede av en standardisering bör områdena trafiksignaler och variabla skyltar standardiseras. Efterhand kan sedan standardiseringen utökas till att omfatta andra områden som används omfattande, exempelvis kan kommunikationen till VViS stationer anslutas. Områden som i dagsläget inte används eller endast används i begränsad omfattning kan standardiseras om de tas i bruk respektive om det är ekonomiskt försvarbart. Även kommunikationen mellan centraler kan standardiseras enligt NTCIP: s standard om det anses motiverat.

Viktigt att tänka på är att NTCIP inte kan tas i bruk rakt av som det är. Ett omfattande arbete krävs för att anpassa det från amerikanske normer och synsätt till svenska/nordiska normer och synsätt. Framförallt är det datainnehållet som kräver bearbetning, i princip kan sägas att det krävs att nya datalexikon tas fram. Enligt personer i branschen är det främst inom området trafiksignaler det krävs ett omfattande arbete, medan övriga områden inte kräver lika omfattande arbete. Exempelvis ska området variabla skyltar principiellt kunna användas som det är.

15 Övrigt

Vägverket bör snarast ta ett beslut i frågan om en standardisering ska genomföras, främst för att leverantörer ska kunna ta fram strategier för deras framtida agerande. Om en standardisering genomförs är det viktigt att Vägverket klarlägger vad man vill uppnå med denna.

För att en standardisering ska genomföras måste det finnas någon som bär kostnaderna. Bristen av incitament för att leverantörerna ska gå ihop och genomföra en standardisering gör att det är upp till beställarna (vägverket och kommuner) om en standardisering ska genomföras. Beställarna blir sannolikt tvungna att bära de kostnader en standardisering medför med avseende på ändringsarbete av standard så att denna passar svenska synsätt och normer samt får ökade kostnader för nya apparater under den första tiden efter standardiseringen. De ökade kostnaderna under den första tiden beror på att leverantörerna behöver utveckla produkter som följer standarden, vilket sannolikt medför en fördyring av apparaterna till en början.

Innan det kan beslutas att en standardisering ska genomföras krävs det att en ekonomisk analys genomförs, så att kostnaderna för en standardisering blir klarlagda. Denna ekonomiska analys bör omfatta kostnader för anpassning av standard, införande av standard och drift med standard. Vilket resultat denna ekonomiska analys ger har stor betydelse för om en standardisering ska genomföras.

Oavsett hur väl skriven specifikation för en standard är kan missförstånd uppstå, på grund av detta är det mycket viktigt att certifiering av produkter genomförs. Detta för att garantera att produkterna följer standarden och kan interopera tillsammans med övriga produkter som gör det. För detta ändamål är det lämpligt att någon typ av certifieringsinstitut med passande testprocedur inrättas.

16 Resultat

Den problembild som finns beroende på användandet av flera olika protokoll för kommunikation är önskevärd att upphäva. Detta går endast att göra genom en standardisering. En standardisering av kommunikation till och från centraler och fältapparater bör ske vid rimliga kostnader för ett genomförande. Största anledningarna till att en standardisering bör ske är fördelarna med interoperabilitet och utbytbarhet av apparater, vilket gör att monopol och leverantörsberoende kan undvikas samt att en rättvisare konkurrenssituation understöds.

Viktigt är att en ekonomiskanalys utförs, som ger svar på långsiktig ekonomisk påverkan samt ett kostnads/nyttoförhållande. Långsiktigt kan det vara ekonomiskt lönsamt med en standardisering, då samordningsvinster finns för främst nätverk samt att förutsättningarna förbättras för en kraftigare pris- och kvalitetskonkurrens. En standardisering bör ske även om det är höga kostnader, då fördelarna är gynnsamma. Tidpunkten för en standardisering anses vara i läget att en standardisering bör ske snarast eller inte alls.

En standardisering bör omfatta så många ITS-områden som möjligt, då detta leder till större samordningsmöjligheter för nätverk och data. Viktigt är främst att området trafiksignaler omfattas, men även området variabla skyltar bör omfattas. Övriga områden är önskvärda men ej lika viktiga. Standarden bör ej begränsa framtida områden och applikationer. Realistiskt är att börja med att standardisera kommunikation för områdena trafiksignaler och variabla skyltar för att beroende på behov, vilja och ekonomiska förutsättningar standardisera övriga områden.

Ur teknisk synvinkel rekommenderas att både bärprotokoll och datainnehåll standardiseras. Standardiseras endast ett av dessa två områden uppnås inte full interoperabilitet och utbytbarhet av apparater. Viktigt är att TCP/UDP och IP stöds, då det ger en mängd möjligheter med avseende på utnyttjande av befintliga nätverk.

För att en standardisering ska få tillräcklig genomslagskraft bör fler länder än Sverige omfattas av den. Lämpligt är försöka få med övriga nordiska länder i standardiseringen, då dessa har liknande signaltekniska traditioner som Sverige. Vilka branschaktörer som bör medverka beror till stor del på vilken typ av standardisering som ska genomföras och bör fastställs i ett senare skede.

En ny standard bör inte utvecklas för en standardisering. Optimalt är att använda en redan befintlig standard med ITS-anknytning som når upp till de krav som ställs på en standard, då detta leder till mindre arbete och lägre kostnader. Om ingen standard finns som uppfyller de krav som ställs bör den bäst lämpade standarden användas som bas för vidareutveckling av en ny standard. Krävs vidareutveckling kan eventuellt en standard från produktionsindustrin vara bättre lämpad än en standard med ITS-anknytning.

Efter att ha jämfört aktuella standarder med de rekommendationer som gjorts framkom att den amerikanske standarden NTCIP är den bäst lämpade standarden att använda vid en standardisering. NTCIP är den enda standard som omfattas av denna rapport som uppfyller de rekommendationer som gjorts om vilka egenskaper en ITS-standard bör ha. Samtliga tänkbara ITS-områden omfattas av NTCIP, detta möjliggör att område efter område kan standardiseras efterhand beroende på behov, vilja och ekonomiska förutsättningar. NTCIP omfattar även områden som inte direkt berör denna rapports syfte som kommunikation mellan centraler.

Viktigt att tänka på är att NTCIP inte kan tas i bruk rakt av som det är. Ett omfattande arbete krävs för att anpassa det från amerikanske normer och synsätt till svenska/nordiska normer och synsätt. Framförallt är det datainnehållet som kräver bearbetning. Enligt personer i branschen är det främst inom området trafiksignaler det krävs ett omfattande arbete, medan övriga områden inte kräver lika omfattande arbete.

17 Övriga kommentarer

Ämnet som berörs av denna rapport är knivigt. Det är ytterst få personer som har helhetsbild över ämnet och flera av dessa personer innehar sådana positioner så att de sannolikt delger delvis partiska åsikter. Vissa problem finns även med att personer verksamma i delområden saknar helhetssyn. En del av arbetet har varit att genomskåda när åsikter finns endast för att de gynnar den enskilda personen, det enskilda företaget eller när helhetssyn saknas.

Försök har gjorts för att undersöka vad som görs i de stora länderna i Europa, men inget av betydelse har framkommit.

De rekommendationer som gjorts är på en strategisk nivå. Vilket gör de eventuellt är orealistiskt att uppfylla samtliga vid en standardisering. Eventuellt kan även någon rekommendation anses onödig eller till och med icke korrekt av visa personer, då vissa rekommendationer endast bygger på ett fåtal personers uppfattningar.

Eventuellt kan det finnas några felaktigheter i beskrivningarna av aktuella protokoll och standarderpå grund av att informationen om dessa är på andra språk. Mestadels har informationen om standarderna varit på engelska, vilket inte anses vållat några problem. För de tyska standarderna OCIT och TLS finns endast information tillgänglig på tyska. Detta har främst medfört att dessa standarder tagit längre tid att fördjupa sig i. I vilket fall som helst är detta inget som påverkar de rekommendationer som gjorts, men det ska finnas i åtanke vid ingående studier av bilagorna.

18 Rekommenderad vidaregång

Personer som arbetar med ITS på Vägverket bör snarast kontakta med de personer som arbetar med trafiksignaler på Vägverket om den undersökning som pågår angående standardisering inom trafiksignalområdet för norden. Utmynnar denna kontakt positivt och en standardisering blir aktuell bör denna rapports rekommendationer beaktas.

Är de verksamma inom trafiksignalområdet inte positiva till en standardisering bör en standardisering ske med området variabla skyltar i fokus. Detta främst för att uppnå utbytbarhet av apparater. Samma rekommendationer bortsett från att området trafiksignaler ska omfattas gäller då.

Viktigt är att det inom en förhållandevis snar framtid beslutas om en standardisering ska ske, beslutet bör sedan förmedlas till berörda aktörer snarast möjligt.

19 Källförteckning

19.1 Hemsidor

http://www.canopen.org
http://www.infrasite.nl/index_astrin.htm
http://www.modbus.org
http://www.ntcip.org
http://www.ocit.org
http://www.profibus.org
http://www.siemens.com/page/1,3771,226865-0-999_0_0-0,00.html

19.2 Dokument

Dokumentnamn	**Dokumentbeteckning**
Einführung in das System	OCIT-O-System_V1.0
Regeln und Protokolle	OCIT-O-Protokoll_V1.0
Basisdefinitionen für Feldgeräte	OCIT-O-Basis_V1.0
Lichtsignalsteuergeräte	OCIT-O-Lstg_V1.0
Profil 1 – Übertragungsprofil	OCIT-O- Profil_1_V1.0
Einführung in das System	OCIT-O-System_V1.0
NTCIP Transportation Management Protocol (TMP)	1103
NTCIP CORBA Naming Convention Specification	1104
NTCIP CORBA Security Service Specification	1105
NTCIP SP-PMPP/FSK	2102
NTCIP TP-Transportation Transport Profile	2201
NTCIP AP-DATEX-ASN	2304
NTCIP AP-CORBA	2305
NTCIP InP-CORBA	2502
NTCIP Guide	9001
IVERA Functional Specification	V 1.30
Modbus Application Protocol Specification	V1.1
Modbus Messaging on TCP/IP Implementation Guide	Rev 1.0
Modbus over Serial Line Specification & Implementation Guide	vV1.0
Profibus Teknologi och Användning	Profibus 4002 vAugust2002-swedish
PROFInet Technology and Application	Profibus 4132 dSeptember2003-english
Technische Lieferbedingungen für Streckenstationen (TLS)	Aufgabe 2002
Description for FuturitCom Chain Driver Protocol	ChainCom.doc v1.3

19.3 Böcker

The Design of Everyday Things, Donald A. Norman, MIT Press, 1998, ISBN: 0262640376
Datakommunikation nu och i framtiden, Magnus Ewert, Studentlitteratur, 1998, ISBN: 91-44-01252-7

19.4 Personer

Nedan listas personer som kontaktas under arbetet.

Benny Ahlqvist, Stunt AB, Umeå
Jonny Alf, Vägverket, Borlänge
Bengt Anderberg, Lumilite AB, Malmö
Åke Andersson, Balanz, Stockholm
Svante Berg, Vägverket, Borlänge
Janne Björk, Stockholm Stad, Stockholm
Karl-Lennart Bång, Kungliga Tekniska Högskolan, Stockholm
Michael Cewers, Swarco Sverige AB, Stockholm
Set Eriksson, Focus Neon AB, Stockholm
Joakim Fredriksson, Vägverket, Borlänge
Ola Hagring, Trivector, Lund
Bengt Hallström, Vägverket, Borlänge
Bjarne Holmgren, Vägverket, Kristianstad
Knut Heijkenskjöld, Vägverket, Borlänge
Patrik Jonason, Aerotech Telub, Östersund
Peter Kronborg, Movea, Stockholm
Mats Lundström, Vägverket, Borlänge
Mats Månsson, Peak Traffic AB, Stockholm
Tomas Olsson, Vägverket, Göteborg
Thorvald Paulsen, Scanmatic AS, Norge
Alf Peterson, Vägverket, Stockholm
Torsten Rose, Safe Trafic Scandinavia AB, Karlstad
Jan Rosenqvist, Vägverket, Göteborg
Clas Rydergren, Linköpings Universitet, Norrköping
Thorsten Schneider, Niechoj electronic GmbH, Tyskland
Stellan Tengroth, Vägverket, Göteborg
Peter Wessel, Vägverket, Göteborg
Peter Wenter, Systemberatung Straßenverkehrstechnik, Tyskland
Jan Zanen, Stiftelsen Beheer Ivera Protocol, Holland
Di Yuan, Linköpings Universitet, Norrköping

20 Figur- och tabellförteckning

21 Bilaga 1

21.1 OSI-modellen

Open System Interconnection (OSI) modellen skapades av International Organization for Standardization (ISO) i början av 80-talet för att strukturera implementeringen av protokoll och tjänster i datanätverk. Trots att nätplattformarna skiljer sig markant åt vad gäller uppbyggnad av tjänster och funktionsomfattning så är OSI-modellen vitt accepterad för att sortera kommunikationsprotokoll och dess enskilda funktioner. OSI-modellen består av sju olika skikt som har olika uppgifter. I tabell 6 ses de olika skikten med respektive uppgift.

Skikt	Uppgifter	Funktioner
Applikationsskiktet (7)	Förser användarna med nätverkstjänsterna. Servrarna broadcastar nätverkstjänsterna.	Nätverks tjänster Tjänst tillkännagivande
Presentationsskiktet (6)	Översätta data till gemensam syntax samt kryptera/dekryptera data	Översättning Kryptering
Sessionsskiktet (5)	Initierar kommunikationen. Etablerar, upprätthåller och synkroniserar dialog mellan enheter	Dialog kontroll Session administration
Transportskiktet (4)	Delar upp meddelanden i mindre paket eller slår samman i större paket. Sätter i rätt ordning, d.v.s. End-to-End realability	Adress resolution Adressering Segment utveckling
Nätverksskiktet (3)	Flyttar data mellan oberoende nätverk. Routing. Flyttar data till specifika IP-adresser. Internetworking.	Adressering Rutt finnande Rutt val
Datalänk skiktet (2)	Organiserar det fysiska skiktets bitar i frames. Upptäcker och korrigerar fel. Kontrollerar dataflödet. Identifierar datorer på det lokala nätverket.	Logisk topologi Transmissions-synkronisering
Fysiska skiktet (1)	Definierar nätverkets fysiska struktur. Definierar mekaniska och elektriska specifikationer för användning av transmissionsmediet. Definerar hur databitar kodas och när mottagaren ska mäta signalen.	Kontakt typer Fysisk topologi Signalering

Tabell 6 OSI-skikt med respektive uppgift och exempel på funktioner (källa: http://home2.swipnet.se/~w-24488/osimodel.htm med vissa förändringar)

En överföring använder normalt minst ett protokoll från varje skikt. Serien av protokoll som används i en överföring kallas protokollstack. Om ett kommunikationssystem inte behöver vissa funktioner har motsvarande skikt ingen funktion och hoppas över.

Det är möjligt för ett par apparater att utväxla meddelanden fast de inte använder samma protokollstack, om protokollstackarna skiljs åt i endast ett eller två skikt eller i de lägre skikten. För att detta ska vara möjligt krävs en likartad definition av datainnehållet.

22 Bilaga 2

Nedan beskrivs världsstandarder från produktionsindustrin som inom ITS-området främst används för styrning av variabla skyltar. Informationen om standarderna har inhämtas från respektive standards bakomliggande organisation, på grund av detta är informationen mer eller mindre partisk och brister kan ha undanhållits.

22.1 CANopen

CANopen är ett standardiserat applikationsskiktsprotokoll optimerat för inneslutna nätverk (främst Controller Area Network, CAN). Huvudsakligen används det i inneslutna låg- och medelvolymssystem, men det finns även implementerat i automatiseringskontrollsystem. I de lägre skikten används CAN protokollet.

22.1.1 Omfattning

CANopens specifikationer täcker applikationsskikt och kommunikationsprofil, så väl som struktur för programmerbara apparater, rekommendationer för kablar, kontakter för/i SI enheter och prefix representationer.

22.1.2 Medverkande

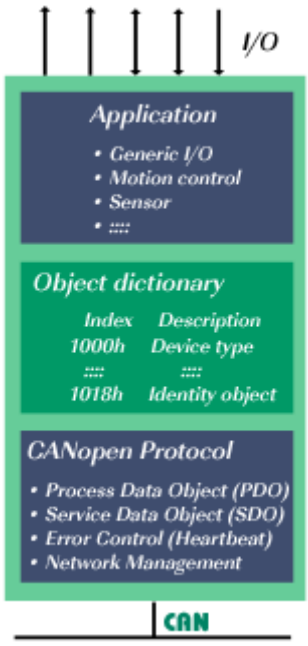
CANopen och CAN är framtaget av CAN in Automation (CiA) som är användare och leverantörers internationella organisation, i dagsläget har CiA 565 medlemmar. CiA utvecklar och stödjer CAN-baserade protokoll ur de högre skikten i OSI-modellen. Alla aktiviteter är baserade på CiA medlemmars intresse, deltagande och initiativ. CiA representanter stödjer aktivt standardisering av CAN protokoll och representerar medlemmarnas intressen i nationella och internationella standardiseringsorganisationer, som ISO och IEC. Medlemmarna i CiA initierar och utvecklar specifikationer som sedan publiceras som CiA standarder. Dessa specifikationer täcker fysiskaskiktets definitioner såväl som applikationsskiktets och utrustningsprofilbeskrivningar.

22.1.3 Kommunikationsmodell

Alla CANopen apparater kan ses på samma sätt, apparaterna är anslutna till CAN på ena sidan och till applikationsspecifika I/O data på den andra sidan (se figur 8). Gränssnittet mellan applikation och CAN är realiserat av ett objektlexikon. Objektlexikonet är unikt för varje CANopen apparat och representerar hela accessen till dess implementerade applikation i form av data och konfiguration. För att få access till objektlexikonet måste varje CANopen apparat realisera en CANopen protokollstack. Denna CANopen protokollstack är en del av mjukvaran, som normalt är implementerad i samma kontrollerare som används av applikationsmjukvaran.

CANopen protokollstacken består av olika funktioner för olika ändamål.

- Process Data Object (PDO) används för att överföra applikationsdata. Applikationsdata överförs utan någon protokollheader (frame) i Broadcast.
- Service Data Object (SDO) används för att få access till en apparats alla parametrar och för direkt apparat till apparat kommunikation.
- Felkontroll används för att validera att alla apparater fungerar ordentligt vad gäller dess CANopen kommunikation.
- Nätverksmanagement används för att kontrollera nätverket vad gäller CANopen kommunikation och indirekt i form av systemuppförande.



Figur 8 CANopen kommunikationsmodell (Källa: www.canopen.org)

CAN

CAN är ett seriellt bussystem speciellt anpassat för att koppla ihop intelligenta apparater för att skapa intelligenta system eller subsystem. CAN: s viktigaste egenskaper är följande:

- Multimaster förmåga, vilket gör att intelligenta och redundanta system kan byggas utan behov av en dyr master
- Användandet av Broadcast meddelande
- Sofistikerad feldetekteringsmekanism och återöverföring av felaktiga meddelanden

CAN protokollet

CAN protokollet är en internationell standard definierad i ISO 11898.

Logik

CAN är baserat på Broadcast kommunikation. Broadcast kommunikation uppnås genom användning av ett meddelandeorienterat överföringsprotokoll, som inte definierar stationer och stationsadresser, utan enbart definierar meddelanden. Meddelandena identifieras genom

användning av meddelandeidentifiering. Ett meddelandes identifieringsnummer måste vara unikt i hela nätverket. Identifieringsnumret definierar meddelandets innehåll och prioritet.

En hög nivå av system- och konfigurationsflexibilitet uppnås som resultat av det innehållsorienterade adresschemat. Det är enkelt att ansluta stationer till ett existerande CAN nätverk utan att behöva göra hård- eller mjukvaru modifieringar i de existerande stationerna så länge som de nya stationerna är rena mottagare. CAN protokollet stödjer multipelt mottagande och synkronisering av processer. De stationer som mottar data behöver inte veta vem som producerat den. Detta gör att det är enkelt att serva och uppdatera nätverket då dataöverföringen inte är baserad på tillgängligheten av en viss specifik typ av station.

Meddelandenas prioritet bestämmer i vilken ordning de skickas, varje meddelandes identifieringsnummer specificerar dess prioritet. Prioriteterna bestäms under systemdesignen i form av korresponderande binära värden och kan inte ändras dynamiskt. De meddelanden med lägst binärt nummer som identifiering är de med högst prioritet.

Bussaccess konflikter löses genom bitvis åtskiljande av de identifierare som är involverade genom att varje station observerar bussnivån bit för bit. Detta sker i överensstämmelse med ”wired and” mekanismen, i vilken den dominerande statusen skriver över den recessiva statusen. Tävlingen om bussen förloras av alla stationer med recessiv överföring och dominant observation. Dessa förlorare blir automatiskt mottagare av det meddelande med högst prioritet och försöker inte överföra igen förrän bussen är tillgänglig på nytt.

Frames

CAN protokollet stödjer två typer av meddelande frames, den huvudsakliga skillnaden dem emellan är storleken på identifieringen. Den såkallade CAN standard frame stödjer en längd på 11 bitar för identifieringen medan den såkallade CAN utbredd frame stödjer en längd på 29 bitar för identifieringen.

Säkerhet

Olikt andra bussystemsprotokoll använder sig inte CAN protokollet av bekräftande meddelanden utan istället signaleras ett fel direkt när det förekommer. Bekräftandet fungerar så att biten i ACK fältet i framen skickas som en recessiv bit och skrivs över till en dominant bit av de mottagare som mottagit data korrekt. För fel detektion har CAN protokollet tre mekanismer implementerade på meddelandenivå:

- Cyclic Redundancy Check (CRC) säkerställer informationsinnehållet i framen genom att lägga till extra kontrollbitar. Mottagaren kontrollerar med hjälp av dessa bitar om bitarna i meddelandet förändrats.
- Frame check verifierar den överförda framens struktur genom att kontrollera bit fälten jämfört med det fastställda formatet och framestorleken.
- ACK errors indikerar att ett ACK fel uppstått om ingen bekräftelse är mottagen av sändaren.

CAN protokollet implementerar även två mekanismer för fel detektering på bit nivå:

- Monitoring, varje station som överför meddelanden observerar bussen och upptäcker skillnader mellan de skickade bitarna och de mottagna. Detta medger tillförlitlig detektion av globala fel och lokala fel hos sändaren.
- Bit stuffing. Kodningen av de individuella bitarna testas på bit nivå. För bit representationen använder CAN sig av Non Return to Zero (NRZ) kodning.

Synkroniseringskanter skapas genom utfyllning med extra bitar. Det betyder att efter fem likadana bitar infogar sändaren en skräp bit i bitströmmen. Skräp biten tas bort av mottagaren.

Om ett eller flera fel upptäcks av minst en station genom användande av ovanstående mekanismer avbryts överföringen genom att en fel flagga (error flag) skickas. Detta hindrar andra stationer från att acceptera meddelandet och säkerställer datakonsistensen i nätverket. Efter att en överföring avbrutits på grund av ett felaktigt meddelande försöker sändaren automatiskt att överföra det igen.

En defekt station kan avbryta all överföring av meddelanden (även de korrekta), vilket skulle medföra att hela bussen blockerades. För att förhindra att detta sker tillhandahåller CAN protokollet en mekanism som skiljer sporadiska fel från permanenta fel och defekta stationer. Detta görs genom statistiska uppskattningar av stationsfel situationer med avseende på att identifiera en stations egna defekter och eventuellt ändra operationsläge till ett där det övriga nätverket inte påverkas. Detta kan gå så långt så att en station stänger av sig själv.

Objektlexikon

Objektlexikonet representerar hela accessen till en apparats implementerade applikation i form av data och konfiguration. Objektlexikonet ger access till alla typer av data i apparaten, kommunikationsparametrar (för konfiguration av apparaten i form av kommunikation), applikationsdata och konfigurationsparametrar. I tabell 7 ses objektlexikonets index med beskrivning.

Index	Beskrivning
0000h	reserverad
0001h-0FFFh	datatyper
0260h-1FFFh	reserverad
1000h-1FFFh	kommunikationsobjekt area
2000h-5FFFh	tillverkarspecifik area
6000h-9FFFh	apparatprofilspecifik area
A000h-BFFFh	gränssnittprofilspecifik area
C000h-FFFFh	reserverad

Tabell 7 Objektlexikonets index med beskrivning

CANopen

CANopen stödjer direktaccess till utrustningsparameters och överföring av tidskritiska data. CANopens nätverks managementtjänster förenklar projektdesign, systemintegration och diagnostik. I varje decentraliserad kontrollapplikation krävs olika kommunikationstjänster och protokoll. CANopen definierar dessa tjänster och protokoll såväl som nödvändiga kommunikationsobjekt.

CANopens standardiserar kommunikationsobjekt för realtidsdata (PDO), konfigurationsdata (SDO), specialfunktioner (Time Stamp, Sync message och Emergency message), felkontroll och nätverksmanagementdata. De beskrivs alla nedan.

PDO

PDO är mappade till en CAN frame och använder upp till 8 bytes av datafältet för att överföra applikationsobjekt. Varje PDO har en unik identifierare och överförs av enbart en enhet, men kan tas emot av flera.

PDO överföring

PDO överföringar kan framdrivas på fyra olika sätt: en intern händelse, en intern timer, en begäran från en annan enhet och av ett mottagande av ett Sync meddelande.

- Händelsedriven: När en händelse (specificerad i apparatprofilen) sker, sätts en överföring igång.
- Timerdriven: När timer tiden gått ut sätts en överföring igång. Detta används för periodiska överföringar.
- Begärandriven: En annan apparat initierar en överföring genom att skicka en överföringsbegäran.
- Sync meddelandedriven: För att initiera en simultan sampling av ingångsdata från alla noder krävs ett periodiskt överfört Sync meddelande. Synkron överföring av PDOs kan ske cykliskt och acykliskt. Vid cyklisk överföring väntar enheten tills den fått ett Sync meddelande, när meddelandet mottagits skickar enheten sina ingångsdata. Enhetens PDO överföringstypnummer (1 till 240) indikerar hur många Sync meddelande enheten ska ta emot innan den utför nästa överföring av sina ingångsdata. Acykliska överföringar av PDOs sätts igång av en definierade applikationsspecifik händelse. Enheten överför ingångsdata med nästa Sync meddelande och överför inte igen förrän en annan applikationsspecifik händelse skett.

PDO mappning

Den normala (default) mappningen av applikationsobjekt och det överföringssätt som stöds är beskrivna i objektlexikonet för varje PDO. PDO identifierare ska ha hög prioritet för att garantera en kort responstid. PDO överföringar bekräftas inte. PDO mappningen definierar vilka applikationsobjekt som överförs inom en PDO. Det beskriver sekvens och längd av de mappade applikationsobjekten. En apparat som stödjer variabel mappning av PDOs måste stödja detta under förstadiet till handlingen (Pre-Operational). Om dynamisk mappning stöds under handlingsstadiet är SDO klienten ansvarig för data konsistensen.

SDO

SDO används för att få access till en apparats alla parametrar och för direkt apparat till apparat kommunikation. SDO läser från poster eller skriver till poster i objektlexikonet. SDOs transportprotokoll tillåter överföring av objekt, oavsett objektets storlek. Den första byten innehåller nödvändig flödeskontrollinformation. De följande tre byten av det första segmentet innehåller de index och subindex i objektlexikonet som är redo att läsas eller skrivas till. De efterföljande 4 byten i det första segmentet är tillgängliga för användardata. Det andra och de följande segmenten innehåller kontrollbyten och upp till 7 byte med användardata. Mottagaren bekräftar varje segment eller segmentblock, så att peer-till-peer kommunikation (klient/tjänare) kan ske.

Nätverksmanagement (NMT)

CANopens nätverksmanagement objekt består av Boot-up meddelande, Heartbeat protokollet och NMT meddelande. Heartbeat protokollet beskrivs under rubriken Felkontroll, Boot-up och NMT meddelande beskrivs nedan.

NMT meddelande

NMT meddelandet är mappat till en CAN frame på 2 byte, dess identifiering är 0. Den första byten innehåller kommandospecificeringen och den andra enhets-ID för apparaten som måste utföra kommandot. I de fall enhets-ID är 0 måste alla enheter utföra kommandot. CANopens specificerar statusarna Initialization, Pre-Operational, Operational och Stopped. NMT meddelanden överförda av NMT mastern tvingar enheterna till att växla status. Efter att apparaten satts igång är den i status Initialization, vilket automatiskt ändras till Pre-Operational. Under statusen Pre-Operational tillåts överföring av SDOs. Om NMT master sätter en eller flera enheter i statusen Operational tillåts de överföra och ta emot PDOs. I statusen Stopped tillåts ingen kommunikation förutom den med NMT objekt.

Statusen Initialization är uppdelad i tre delstatusar för att möjliggöra en komplett eller partiell reset av en enhet. I delstatusen Reset Application sätts parametrarna i den tillverkarspecifika profilarean och i den standardiserade apparatprofilarean till deras igångsättningsvärden. I delstatusen Reset Communication sätts parametrarna i kommunikationsprofilarean till sina igångsättningsvärden. I delstatusen initialising, vilket en enhet automatiskt antar efter igångsättning, är igångsättningsvärdena de senast sparade parametrarna.

Boot-up meddelande

En apparat skickar Boot-up meddelandet till NMT mastern för att indikera att den nått statusen Pre-Operational. Detta sker varenda gång apparaten bootar upp och även efter ett strömavbrott under operation. Boot-up meddelandet har samma identifiering som ett Heartbeat objekt men dess datainnehåll är noll.

Felkontroll

För felkontroll används protokollet Heartbeat. Det signalerar närvaron av en nod och dess status. Heartbeat meddelandet är ett periodiskt meddelande från en nod till en eller flera andra noder. Det indikerar att den sändande noden fungerar tillfredställande. Vid sidan av Heartbeat protokollet existerar det en gammal och utrangerad felkontrolltjänst, den kallas Node and Life Guarding protokollet. Det är rekommenderat att inte användas.

Special funktioner

CANopen definierar tre specifika protokoll för synkronisering, nödindikering och time-stamp. De beskrivs nedan.

Synkroniserings objekt

Sync objektet Broadcastas periodiskt av Sync producenten. Tidsperioden mellan Sync meddelandena definieras av kommunikationscykelperioden, som kan nollställas av ett konfigurationsverktyg till applikationsapparaten under boot-up processen. Det kan vara jitter i

överföringen av Sync meddelanden beroende på andra objekt med högre prioritet eller beroende på att en frame överförts precis före Sync meddelandet. Sync meddelandet är mappat till en CAN frame med identifiering 128 och det innehåller ingen data.

Nödindikerings objekt

Nödmeddelanden skickas när det uppstått en intern felsituation och överförs från en nödproducent på den berörda applikationsapparaten. Ett nödmeddelande överförs endast en gång per ”felhändelse”. Noll eller fler nödkonsumenter kan ta emot nödmeddelanden. Nödkonsumentens reaktion är applikationsspecifik. CANopen definierar flera olika nödfelskoder. Nödmeddelandena överförs i en CAN frame på 8 byte.

Time-Stamp objekt

Med avseende på Time-Stamp tillhandahålls en vanlig tidsramsreferens till applikationsapparaterna. Den innehåller ett värde av typen tid-på-dagen. Denna objektöverföring följer producent/konsument push modellen. Den associerade CAN framen har en fördefinierad identifiering på 256 och ett datafält på 6 byte.

22.1.4 Användning

CANopen används inom en mängd olika tillämpningsområden. Huvudområdena är följande:

- Lastbilsbaserade överbyggnadskontrollsystem
- Anläggningsmaskiner
- Passagerar- och godståg
- Marinelektronik
- Fabriksautomatisering
- Industriell maskinkontroll
- Hissar och rulltrapport
- Byggnadsautomatisering
- Medicinsk utrustning
- Icke industri kontroll
- Icke industri utrustning

CAN kan användas i alla dessa områden samt inom följande områden:

- Passagerarfordon
- Lastbilar och bussar
- Flyg- och rymdelektronik

Inom denna rapports berörda ITS-områden används det av det tyska företaget Niechoj electronic GmbH. Niechojs produkter marknadsförs och säljs i Sverige av Lumilite AB.

22.1.5 Tillgänglighet

För tillgång till CiAs standarder krävs medlemskap i CiA. Medlemskap fås mot en medlemsavgift som betalas årsvis. Kostnaden för detta medlemskap varierar från 180 euro för associerade medlemmar (studenter) till 7 500 euro för företag med mer än 100 000 anställda.

22.2 Modbus

Modbus är en industristandard med ursprung från 70-talet. Det används främst för kommunikation mellan automatiseringsutrustningar. Modbus tillhandahåller klient/tjänare kommunikation mellan utrustningar anslutna till olika typer av bussar och nätverk.

22.2.1 Omfattning

Modbus protokollet erbjuder en enkel kommunikation i alla typer av nätverksarkitekturer. Alla typer av anordningar (PLC, HMI, kontrollbord, händelse kontroll, I/O utrustning, med mera) kan använda Modbus protokollet för att initiera operationer. Kommunikation med hjälp av Modbus kan ske seriellt med master/slav, med TCP/IP på ett Ethernet nätverk eller på ett höghastighetsnätverk med en token.

22.2.2 Medverkande

Modbus styrs av en organisation med namnet Modbus. Medlemmar i organisationen är användare och leverantörer av Modbus baserade utrustningar. I dagsläget finns ca 330 företag registrerade som användare av Modbus.

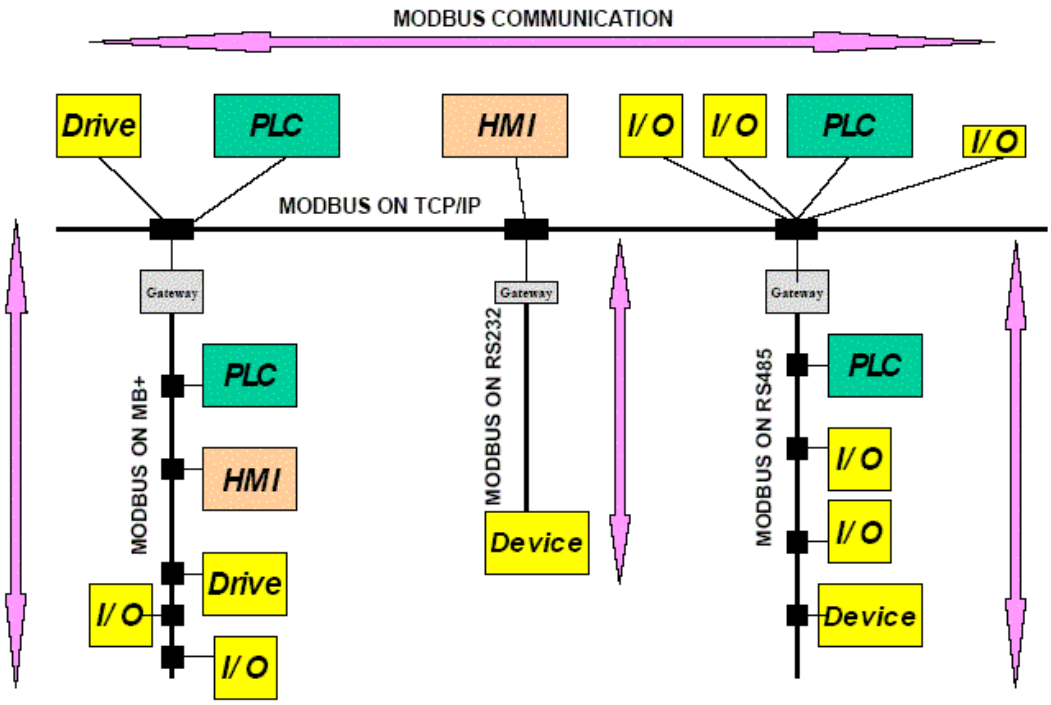
22.2.3 Kommunikationsmodell

Modbusprotokollet tillhör skikt 7 i OSI-modellen. Som tidigare nämnts kan Modbus kommunikation ske på flera olika sätt. I tabell 8 finns en sammanställning över tre kommunikationssätt och deras protokollstackar. Modbus med seriellkommunikation och Modbus med TCP/IP på Ethernet beskrivs mer ingående nedan.

<table>
<tr><th>OSI-skikt</th><th>Modbus med seriellkommunikation</th><th>Modbus med TCP/IP på Ethernet</th><th>Modbus med token</th></tr>
<tr><td>7</td><td>Modbus</td><td>Modbus</td><td>Modbus</td></tr>
<tr><td>6</td><td rowspan="4">Inget</td><td rowspan="2">Modbus on TCP</td><td rowspan="4">Inget</td></tr>
<tr><td>5</td></tr>
<tr><td>4</td><td>TCP</td></tr>
<tr><td>3</td><td>IP</td></tr>
<tr><td>2</td><td>Modbus Serial Line Protocol</td><td>Ethernet</td><td>Modbus+ / HDLC</td></tr>
<tr><td>1</td><td>EIA/TIA-485 alt. EIA/TIA-232</td><td>Valbart</td><td>Valbart</td></tr>
</table>

Tabell 8 Sammanställning av protokoll i Modbus beroende underliggande skikt

De olika protokollstackarna hindrar inte kommunikation mellan utrustningar anslutna via olika protokollstackar, de olika utrustningarna kan kommunicera med hjälp av Gateways.



Figur 9 Exempel på Modbus kommunikation vid olika protokollstackar (Källa: Modbus Application Protocol Specification V1.1 med vissa förändringar)

22.2.4 Modbusprotokollet i skikt 7

Logik

I Modbusprotokollet kallas ramen för Application Data Unit (ADU), delen med data kallas för Protocol Data Unit (PDU). Data i PDU: n är oberoende av underliggande skikt och består av en funktionskod och data. ADU: n består av PDU: n, adress och felkontroll. Mappning av protokollet på specifika bussar eller nätverk kan medföra extra bitar i ADU: n.

ADU: n skapas av klienten som initierar en överföring. När ett meddelande skickas indikerar funktionskoden för tjänaren vilken handling den ska genomföra. Man kan säga att Modbus protokollet skapar en fråga initierad av klienten. Funktionskoden är kodad i en byte. Tillåtna koder är från 1-255, men av dessa koder är 128-255 reserverade för avvikande respons. Subfunktionskoder läggs till vissa funktionskoder för att definiera multipla handlingar.

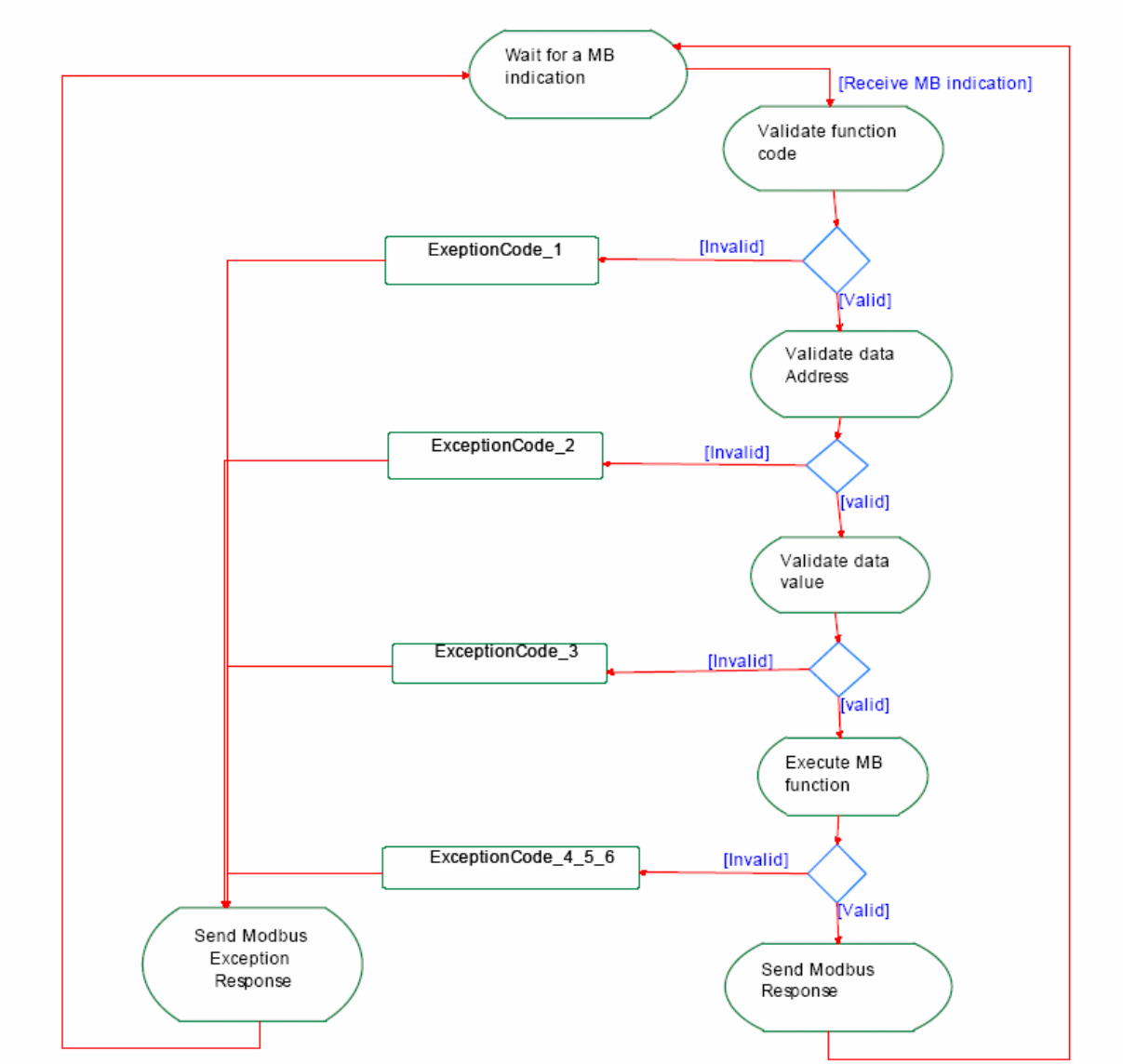
Datafältet i meddelandet skickat från klient- till tjänarutrustning innehåller extrainformation som tjänaren använder för att genomföra den handling som definieras av funktionskoden. Extrainformationen kan exempelvis vara distinkta adresser, register adresser, kvantiteten av poster som kan hanteras och värdet på de faktiska databyten i fältet. I de fall när ingen extrainformation krävs är datafältet tomt.

Om inget fel uppstår relaterat till den funktion som är efterfrågad innehåller svaret från tjänaren den data som efterfrågats av klienten. Vid ett fel relaterat till den efterfrågade funktionen innehåller datafältet en undantagskod som tjänarapplikationen kan använda för att avgöra vilken nästa handling den ska göra är. De olika undantagskoderna redovisas i tabell 9.

Funktionskoden används av tjänaren till att indikera antingen ett normalt (felfritt) svar eller att något fel har skett. För ett normalt svar skickar tjänaren tillbaka original funktionskoden. För ett svar där något gått fel svarar tjänaren med en kod som är som original funktionskoden där den mest signifikanta biten är satt till 1.

Kod	*Namn*	*Betydelse*
01	*Illegal funktion*	*Den mottagna funktionskoden är inte tillåten handling för tjänaren (slaven)*
02	*Illegal dataadress*	*Den mottagna dataadressen är inte tillåten för tjänaren (slaven)*
03	*Illegalt datavärde*	*Ett mottaget datavärde är inte tillåtet för tjänaren (slaven)*
04	*Slavapparat fel*	*Ett orättbart fel uppstod medan tjänaren (slaven) försökte utföra den efterfrågade handlingen*
05	*Bekräftelse*	*Tjänaren (slaven) har accepterat frågan och bearbetar den, men det kommer ta lång tid. Detta svar skickas för att hindra timeout hos klienten (mastern).*
06	*Slavapparat upptagen*	*Tjänaren (slaven) är upptagen med en bearbetning som tar lång tid. Klienten (slaven) ska återkomma med sin fråga senare.*
08	*Minnesparitets fel*	*Tjänaren (slaven) försökte läsa filen men upptäckte ett paritets fel i minnet. Klienten (mastern) kan försöka igen men eventuellt krävs en service av tjänaren (slaven)*
0A	*Gateway väg oanträffbar*	*Indikerar att Gatewayen inte kunde lokalisera en intern kommunikationsväg från inputporten till outputporten för bearbetning av frågan.*
0B	*Gateway målapparaten misslyckades att svara*	*Indikerar att ingen respons nåddes från målapparaten.*

Tabell 9 Undantagskoder i Modbus (Källa: Modbus Application Protocol Specification V1.1 med vissa förändringar)



Figur 10 Modbus överföringsdiagram, MB står för Modbus Protokoll (Källa: Modbus Application Protocol Specification V1.1 med vissa förändringar)

Funktionskodtyper

Det finns tre typer av funktionskoder, publika, användardefinierade och reserverade. Av det totala antalet tillåtna funktionskoder (1-127) är nr 1-64, 73-99 och 111-127 publika funktionskoder och nr 65-72 och 100-110 användardefinierade funktionskoder.

Publika funktionskoder

- Är väl definierade funktionskoder
- Garanterat unika
- Validerade av modbus.org: s Community
- Publikt dokumenterade
- Har tillgängliga ”conformance” test
- Är dokumenterade i Modbus IETF RFC

- Inkluderar både fastlagda definierade publika funktionskoder och icke fastlagda funktionskoder reserverade för framtida bruk

Användardefinierade funktionskoder

- Användare kan välja och implementera en funktionskod utan godkännande från modbus.org
- Det är ingen garanti att användandet av den valda funktionen är/blir unikt
- Om en användare vill repositionera funktionaliteten som en publik funktionskod, måste denna få RFC till att introducera ändringen till den publika kategorin och få en ny publik funktionskod tilldelad.

Reserverade funktionskoder

Funktionskoder som används av några företag för rättsliga produkter och inte är tillgängliga för publikt användande.

Data kodning

Modbus använder sig av en ”big-Endian” representation för adresser och dataposter. Med detta menas att när en numerisk kvantitet större än en byte överförs skickas den mest signifikanta byten först.

Datamodell

Modbus baserar sin datamodell på en serie av tabeller som har utmärkande karaktär. De fyra primära tabellerna ses i tabell 10.

Primära tabeller	***Objekt typ***	***Typ av access***	***Kommentar***
Discrete input	*en bit*	*endast läs*	*Denna datatyp kan tillhandahållas av I/O system*
Coils	*en bit*	*läs och skriv*	*Denna datatyp kan förändras av applikationsprogram*
Input registers	*16-bitars ord*	*endast läs*	*Denna datatyp kan tillhandahållas av I/O system*
Holding registers	*16-bitars ord*	*läs och skriv*	*Denna datatyp kan förändras av applikationsprogram*

Tabell 10 Primära tabeller (Källa: Modbus Application Protocol Specification V1.1 med vissa förändringar)

För varje primär tabell tillåter protokollet individuellt val av 65 536 dataposter. Operationerna för att läsa och skriva dessa poster är designade för att kunna göra detta på multipla efter varandra följande dataposter upp till en datastorleksbegränsning som bestäms av överföringens funktionskod.

All data som hanteras via Modbus måste lokaliseras i apparatapplikationsminnet. Det finns flera olika sätt att organisera data i apparaterna. För varje apparat kan fastställas en egen dataorganisation beroende på dess applikation.

Adresserings modell

Modbus applikationsprotokoll definierar exakta PDU adresseringsregler. I PDU är all data adresserad från 0 till 65 535. Varje element i ett datablock (exempelvis den primära tabellen Coils) är numrerade mellan 1 och n. Mappningen från Modbus datamodell till apparatapplikation är apparatspecifik.

22.2.5 Modbus med seriellkommunikation

I Modbus med seriellkommunikation används inga protokoll i OSI-modellens skikt 3-6. I skikt 2 används Modbus Serial Line Protocol som är ett master/slav protokoll och i skikt 1 används EIA/TIA 485 (RS485) eller EIA/TIA 282 (RS282). I Modbus seriellkommunikation är mastern klient och slaven tjänare.

Logik

En master och mellan 1 och 247 slavenheter är anslutna till en och samma buss. Kommunikation är alltid initierad av mastern. En slav överför aldrig data utan att en begäran mottagits från masterenheten. Slavenheterna kommunicerar aldrig med varandra. Mastern initierar en överföring åtgången. Mastern utfärdar begärningar till slavarna på två sätt:

- Unicast, mastern adresserar en slav. Efter att ha mottagit och bearbetat begärningen svarar slaven med ett returmeddelande. Varje slav måste ha en unik adress (från 1 till 247) så att den kan adresseras oberoende av övriga enheter. När slaven svarar mastern sätter den in sin egen adress i adressfältet.
- Broadcast, master skickar en begäran till alla slavar. Slavarna skickar inget returmeddelande till mastern. Broadcast meddelandena är nödvändigtvis skrivkommandon och adressen 0 används för att identifiera dem.

Adresseringsregler

Adresseringsutrymmet består av 256 olika adresser. Adress 0 används för Broadcast, adress 1 till 247 för unika slavadresser och adress 248 till 255 är reserverade. Alla slavar måste känna till Broadcastadressen. Mastern har ingen adress.

Meddelande beskrivning

I Modbus applikationsprotokoll definieras en PDU med tillhörande ADU. I Modbus seriell line protokollet tas denna PDU emot utan ADU, istället för ADU läggs ett adressfält innehållande enbart aktuell slavadress och ett fält för felkontroll till. För felkontroll används

antingen Cyclic Redundency Checking (CRC) eller Longitudinal Redundancy Checking (LRC) beroende på vilken överföringsstil som används. CRC och LRC beskrivs nedan.

Seriella överföringsstilar

I Modbus är två olika stilar av seriell överföring definierade, Remote Terminal Unit (RTU) stil och American Standard Code for Information Interchange (ASCII) stil. De definierar bitinnehållet hos meddelanden överförda seriellt. De fastställer hur information är packad in i meddelandefält och hur den ska tolkas.

Överföringsstil och seriella portparameters måste vara de samma för alla apparater på en Modbus serielledning. För att interoperabilitet ska kunna uppnås måste alla apparater på en ledning ha samma överföringsstil. Apparaterna iordningställs av användaren till önskad överföringsstil, standard setup måste vara RTU stil. ASCII överföringsstil är ett tillval.

När en apparat använder sig av RTU stil innehåller varje 8-bitars byte i ett meddelande två 4-bitars hexadecimala tecken. Huvudfördelen med RTU stilen jämtemot ASCII stilen är den högre teckendensiteten som medför ett bättre genomflöde av data vid samma baud rate. Varje meddelande måste överföras som en kontinuerlig ström av tecken.

När en apparat använder sig av ASCII stil kodas varje 8-bitars byte som två ASCII tecken. Denna stil används när den fysiska kommunikationslänken eller apparatens egenskaper inte tillåter kraven RTU stil har för timer ledning.

Vid användning av RTU stil används CRC för felkontroll. Ett CRC fält med ett 16-bitars värde läggs till sist i varje meddelande. CRC kontrollerar innehållet i hela meddelandet. CRC värdet beräknas och läggs till meddelandet av den sändande apparaten. Den mottagande apparaten beräknar om CRC värdet under mottagandet av meddelandet och jämför det beräknade värdet med det mottagna värdet i CRC fältet. Om de två värdena inte är lika har ett fel uppstått.

Vid användning av ASCII stil används LRC för felkontroll. Ett LRC fält med ett 8-bitars värde läggs till sist i varje meddelande. LRC kontrollerar innehållet i hela meddelandet bortsett från en inledande extra frame och en avslutande extra frame. LRC värdet beräknas och läggs till meddelandet av den sändande apparaten. Den mottagande apparaten beräknar om LRC värdet under mottagandet av meddelandet och jämför det beräknade värdet med det mottagna värdet i LRC fältet. Om de två värdena inte är lika har ett fel uppstått.

22.2.6 Modbus med TCP/IP

Allmänt

Modbus tillhandahåller klient/tjänare kommunikation mellan apparater anslutna till ett Ethernet TCP/IP nätverk. Klient/tjänare modellen är baserad på fyra typer av meddelanden, Modbus begäran, Modbus indikering, Modbus respons och Modbus konfirmation.

- En Modbus begäran är begäransmeddelandet som skickas till nätverket av klienten för att initiera en överföring.

- En Modbus indikering är begäransmeddelandet mottaget av tjänaren.
- En Modbus respons är svarsmeddelandet som skickas av tjänaren.
- En Modbus konfirmation är svarsmeddelandet mottaget av klienten.

Meddelande uppbyggnad

I Modbus kommunikation över ett TCP/IP nätverk är meddelandeuppbyggnaden annorlunda. Till PDU: n läggs en header med enhetsidentifierare Enhetsidentifieraren används för kommunikation via apparater som gateways och routers, som använder en IP-adress för att stödja multipla självständiga Modbus enheter.

Alla begärningar och svar i Modbus är designade så att mottagaren kan kontrollera att ett meddelande är slut. För funktionskoder där PDU: n har en fastställd längd räcker det med funktionskoden för att mottagaren ska veta hur långt meddelandet är. För funktionskoder som har variabeldatamängd i svar eller begäran inkluderas en byte räknare.

När Modbus överförs över TCP finns extra längdinformation i ramen för att ge mottagaren möjligheten att upptäcka meddelandegränser även om meddelandet har blivit delat i flera paket under överföringen. Existensen av både implicita och explicita längdregler och användandet av CRC-32 felkontroll (på Ethernet) resulterar i obefintligt liten chans till oupptäckta fel i ett begärans- eller ett svarsmeddelande.

Frame

Framen i Modbus över TCP/IP är 7 byte stor. De 7 byten består av en överföringsidentifierare på 2 byte, en protokollidentifierare på 2 byte, ett längd fält på 2 byte och en enhetsidentifierare på 1 byte.

Överföringsidentifieraren används för överförings parning, tjänaren kopierar in överföringsidentifieraren från begärningen i svarsmeddelandet. Protokollidentifieraren används för intern systemmultiplexering, Modbus protokollet identifieras av värdet 0. Längdfältet är en byte räknare av de följande fälten, det vill säga enhetsidentifierare och datafält. Enhetsidentifierare används för internsystem routing. Typisk är att den används för kommunikation till en Modbus eller en Modbus+ serielledningsslav genom en gateway mellan ett Ethernet TCP/IP nätverk och en Modbus serielledning. Fältet sätts av Modbus klienten i begärningen och måste returneras med samma värde i svarsmeddelandet av tjänaren.

Förbindelsemanagement

En Modbus kommunikation kräver upprättande av en TCP förbindelse mellan klient och tjänare. Upprättandet av förbindelsen kan aktiveras uttryckligen av användarapplikationsmodulen eller automatiskt av TCP förbindelsemanagement modulen. I det första fallet måste ett applikationsprogramsgränssnitt tillhandahållas i användarapplikationsmodulen som sköter förbindelsen fullständigt. Denna lösning ger flexibilitet åt applikationsprogrammerare men kräver goda kunskaper i TCP/IP. I det andra fallet är TCP förbindelsemanagementet helt dolt för användarapplikationen, som endast

skickar och tar emot meddelanden. TCP förbindelsemanagement modulen är ansvarig för att upprätta nya TCP förbindelser när det krävs.

Implementeringsregler

- Utan ett tydligt användarkrav rekommenderas implementering av det automatiska TCP förbindelsemanagementen.
- Det är rekommenderat att hålla TCP förbindelsen öppnad till mottagande apparat och inte öppna och stänga den för varje överföring. Klienten måste dock vara kapabel att acceptera en begäran från tjänaren om att stänga ner förbindelsen.
- Det rekommenderas att en klient öppnar ett minimum av TCP förbindelse med tjänare (med samma IP adress). En förbindelse per applikation kan vara en bra nivå.
- Flera överföringar kan aktiveras samtidigt på samma TCP förbindelse. Att tänka på här är att överföringsidentifieringen måste användas för att identifiera matchande begärningar och svar.
- I fall med kommunikation i båda riktningarna mellan två enheter (båda är klient och tjänare), är det nödvändigt att ha separat kommunikation för klient dataflödet respektive tjänar dataflödet.
- En TCP frame får överföra endast en Modbus ADU

22.2.7 Användning

Modbus används främst för industriell kommunikation och automatisering. Inom ITS-området används det av det tyska företaget Niechoj electronic GmbH. Niechojs produkter marknadsförs och säljs i Sverige av Lumilite AB.

22.2.8 Tillgänglighet

Det finns olika typer av medlemskap med skilda kostnader beroende på företagsstorlek och intresse.

22.2.9 Övrigt

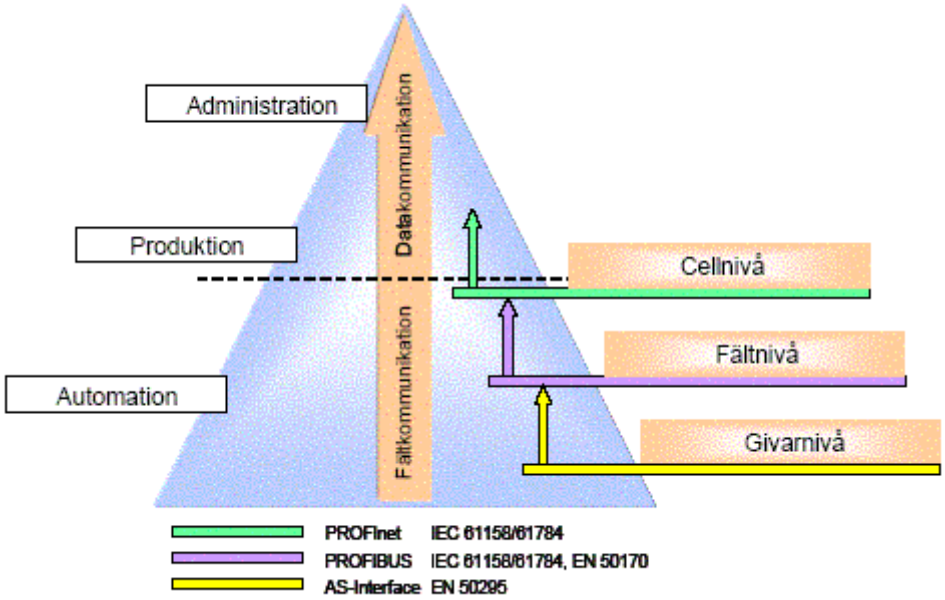
Schneider Automation har lämnat in Modbus TCP/IP protokollspecifikation till Internet Engineering Task Force (IETF) för att uttrycka sitt engagemang för en helt öppen teknologi och för att komma närmare en etablering av Modbus som industrins Internetprotokoll.

22.3 Profibus

Profibus är ett öppet enhetligt digitalt kommunikationssystem som kan användas i så gott som alla automationsområden, i verkstadsindustrin och processautomation i synnerhet men även i trafikstyrning, kraftproduktion och –distribution. Profibus kommunikation är förankrad i de internationella standarderna IEC 61158 och IEC 61784.

22.3.1 Omfattning

Profibus erbjuder kommunikation för alla verkstads- och processautomation. I figur 11 ses en översikt över kommunikationen i automationsteknologi.



Figur 11 Kommunikation i automationsteknologi (Källa: Profibus Teknologi och användning)

På givarnivå överförs signaler från digitala givare och aktorer på en givarbuss. Lämpligt är en buss med enkel installationsteknik där både strömförsörjning och data överförs. I Profibus används AS-Interface som lämpar sig väl för detta ändamål. För information om AS-Interface hänvisas till facklitteratur.

På fältnivå behövs realtidskommunikation mellan fältenheter, som I/O moduler, transmittrar, drivutrustning, analysinstrument, ventiler och operatörspaneler, och automationssystem. Data ska överföras såväl cykliskt som acykliskt. I Profibus används standarden Profibus för detta ändamål. Profibus beskrivs nedan.

På cellnivå kommunicerar PLC:er och industriPC med varandra och med IT-system i kontorsvärlden. Denna kommunikation sker med standarder som Ethernet, TCP/IP, Intranät och Internet. Informationsflödet kräver stora datapaket och en uppsättning kraftfulla kommunikationsfunktioner. För detta ändamål har Profibus utvecklat det öppna och tillverkaroberoende automationskoncept PROFInet som är baserat på Ethernet. PROFInet beskrivs nedan.

22.3.2 Medverkande

Profibus International som står bakom Profibus är världens största organisation för industriell kommunikation. I dagsläget har organisationen ca 1400 medlemmar. Medlemmar i organisationen kan vara försäljare av hårdvara, mjukvara och system så väl som användare och operatörer, vetenskapliga institut och federationer. Det finns regionala Profibus

organisationer i 23 länder, 21 ackrediterade kompetenscentrum och 7 testlaboratorier för certifieringsarbete.

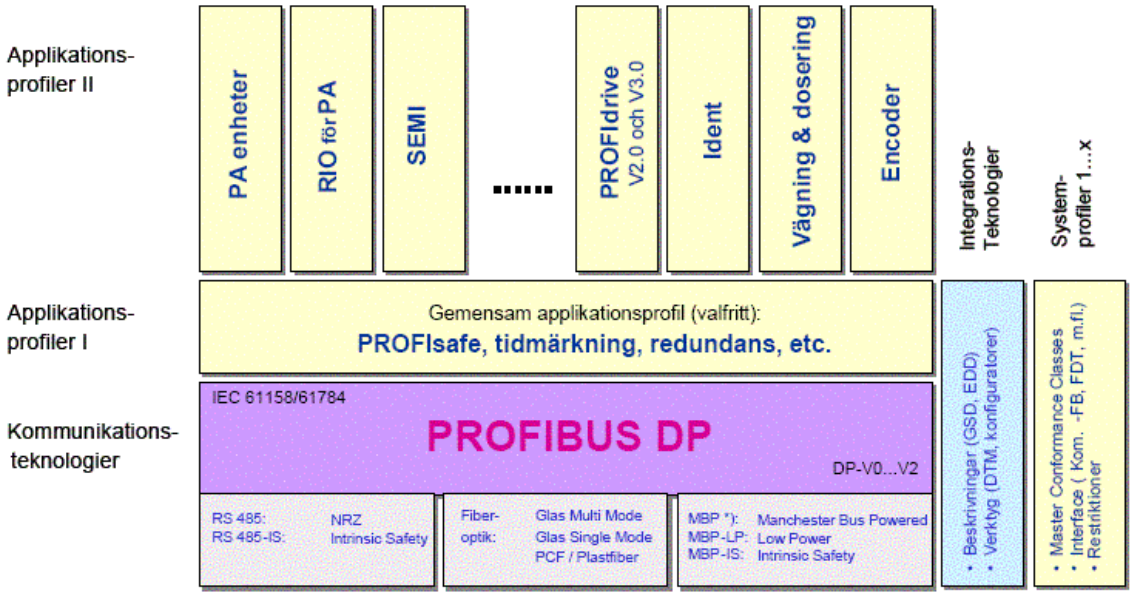
Profibus Internationals huvudsakliga uppgifter är följande:

- Underhålla och utveckla Profibus teknologin
- Utöka acceptansen och användningen av Profibus teknologin
- Skydda användarnas och tillverkarnas investeringar genom att påverka och delta i fortsatt standardisering
- Representera medlemmarnas intresse genom att vara remissinstans för standardiseringskommittéer och organisationer
- Ge teknisksupport över hela världen
- Skapa kvalitetsgaranti genom produktcertifiering

Utvecklingen av Profibus teknologin har överlåtits av Profibus International till den regionala organisationen i Tyskland. Utvecklingsarbetet är organiserat i 5 tekniska kommittéer med mer än 35 permanenta arbetsgrupper. Dessutom finns ett antal extra arbetsgrupper som handhar speciella tidsbegränsade uppgifter. Arbetsgrupperna tar fram specifikationer och profiler, handhar kvalitetsarbetet och standardiseringen, arbetar i standardiseringskommittéer och utför marknadsaktiviteter (mässor, presentationer) för att få Profibus teknologin att växa.

22.3.3 Profibus Kommunikationsmodell

I Profibus standardiseras OSI-modellens skikt 1,2 och 7, i övriga skikt används inga protokoll. Ovanför skikt 7 finns olika typer av profiler, allmänna applikationsprofiler, speciella applikationsprofiler och systemprofiler. Applikationsprofilerna är utformade för specifika produktgrupper och användningsområden. Systemprofilerna beskriver systemklasser, vilket inkluderar funktion, programgränssnitt och hur de ska integreras. I figur 12 ses Profibus systemuppbyggnad för protokoll och applikationsprofiler.



Figur 12 Teknisk systemuppbyggnad för Profibus, applikationsprofiler I är allmänna applikationsprofiler och applikationsprofiler II är speciella applikationsprofiler (Källa: Profibus Teknologi och användning)

22.3.4 Skikt 1

I skikt 1 använder Profibus fyra olika överföringstekniker, MBP, RS485, RS485-IS och fiberoptik. De fyra teknikerna är baserade på internationella standarder. MBP står för Manchester Coding (M) och Bus Powering (BP). I tabell 11 ses en sammanställning över de olika teknikerna och dess egenskaper.

	MBP	RS485	RS485-IS	Fiberoptik
Dataöverföring	Digital, bitsynkron, Manchesterkodning	Digital differentialsignal enligt RS 485 NRZ	Digital differentialsignal enligt RS 485 NRZ	Optisk digital NRZ
Överförings-hastighet	31,25 kBit/s	9,6 till 12000 kBit/s	9,6 till 12000 kBit/s	9,6 till 12000 kBit/s
Datasäkerhet	Telegramhuvud, felsäkra start och sluttecken	HD=4, paritetsbit, start- och sluttecken	HD=4, paritetsbit, start- och sluttecken	HD=4, paritetsbit, start- och sluttecken
Kabel	Partvinnad, skärmad, tvåtrådskabel	Partvinnad, skärmad, tvåtrådskabel av typ A	Partvinnad, skärmad, tvåtrådskabel av typ A	Glas multimod, singelmod, PCF, plast
Energimatning	Kan ske över bussen	Möjligt över extraledningar i kabeln	Möjligt över extraledningar i kabeln	Möjligt med hybridkabel
Explosionsklass	Egensäker (Eex ia/ib)	Nej	Egensäker (Eex ib)	Nej
Topologi	Linje och trädtopo-logi med terminering även kombinerat.	Linjetopologi med terminering	Linjetopologi med terminering	Typiskt stjärn- och ringtopologi, linje är också möjlig
Antal deltagare	Upp till 32 deltagare per segment. Totalt 126 per nät	Upp till 32 deltagare per segment, max 126 med repeatrar	Upp till 32 deltagare per segment. Totalt 126 per nät	Upp till 126 per nät
Antal repeatrar	Maximalt 4 repeatrar	Upp till 9 repeatrar med regenerering	Upp till 9 repeatrar med regenerering	Användarbestämt

Tabell 11 Sammanställning av Profibus överföringstekniker i OSI-modellens skikt 1 (Källa: Profibus Teknologi och användning)

22.3.5 Skikt 2 och 7

I skikt 2 och 7 används det gemensamma protokollet Decentral Periferi (DP). Protokollet har utvecklats för snabbt datautbyte på fältnivå, där centrala programmerbara styrsystem (exempelvis PLC:er, PC och processystem) kommunicerar med decentrala fältenheter (exempelvis ventiler, transmittrar och analysinstrument) via en snabb seriell anslutning. DP är ett master/slav protokoll och finns i tre olika versioner, DP-V0, DP-V1 och DP-V2. Versionerna V0 och V1 innehåller både bindande krav och optioner för implementering, medan version V2 endast specificerar optioner.

DP-V0 omfattar DP:s basfunktioner, inklusive cykliskt datautbyte, stations-, modul- och kanalspecifik diagnostik samt fyra olika typer av avbrott för diagnostik- och processavbrott och för hantering av stationer som tas ur och sätts in i nätverket under drift.

DP-V1 är utökat med inriktning mot processautomation. Den innehåller acyklisk datakommunikation för parametrering, kontroll, visualisering och avbrottshantering av intelligenta fältenheter parallellt med den cykliska datakommunikationen. Detta ger

onlinekontakt med stationer för arbete med ingenjörsverktyg. DP-V1 har även tre tillkommande avbrottstyper statusavbrott, uppdateringsavbrott och tillverkardefinierat avbrott.

DP-V2 är utökat med inriktning mot i förstahand drivteknologi och dess krav. Med hjälp av som synkron slavmod och slav-till-slav kommunikation kan Profibus med DP-V2 användas för reglering av snabba rörelser och sekvenser hos drivaxlar. De olika versionerna beskrivs mer omfattande nedan.

DP-V0

I DP läser mastern cykliskt ingångsinformation och skriver cykliskt utgångsinformation till slavarna. DP överför både ingångsdata och utgångsdata i en enda meddelandecykel. För överföringstjänsten använder sig DP av Send and Request Data with reply (SRD) som tillhör skikt 2 i OSI-modellen.

Adressområdet i DP sträcker sig mellan 0 och 127. Adress 127 används för Broadcasting och adress 126 används normalt till fabriksinställning av slavar som ska erhålla sin adress via bussen. Kvar blir adresserna 0 till 125 vilket gör att maximalt 126 enheter (mastrar och slavar) kan anslutas till bussen.

Vid systemkonfigurationen av DP anges följande:

- Antalet stationer
- Tilldelning av I/O-adresser till stationsadresserna
- Datagrupperingen för I/O-data
- Format för diagnostikmeddelandena
- De bussparametrar som ska användas

Stationstyper

Det finns tre olika typer av stationer i DP, DP master klass 1, DP master klass 2 och slavar.

DP master klass 1 (DPM1)

DPM1 är en master som cykliskt utbyter information med slavarna i en specificerad telegramcykel. Typiska DPM1 stationer är styrsystem (PLC:er) och PC. DPM1-stationer har aktiv access med vilken den kan läsa mätvärden (ingångar) hos fältenheterna och skriva börvärden (utgångar) för aktorerna vid bestämda tidpunkter.

DP master klass 2 (DPM2)

Typiska DPM2-stationer är ingenjörsstationer, konfigureringsverktyg och operatörsstationer. De används för konfigurering, underhåll, diagnostik av anslutna enheter, utvärdering av uppmätta värden och parametrar samt för att läsa status. En DPM2-station behöver inte vara permanent inkopplad till bussystemet.

Slavar

En slav är en fältenhet (I/O terminal, drivutrustning, ventil, HMI-station etcetera) som läser information i processen och/eller använder utgångsinformation för att ingripa i processen. Det

finns även slavar som endast bearbetar ingångs- och utgångsinformation utan att påverka processen.

Mono- och multimastersystem

Både mono- och multimastersystem kan implementeras i DP. I monomastersystem är endast en master aktiv när bussen är i drift. I ett multimastersystem är flera mastrar anslutna till bussen. De är antingen oberoende styrsystem med varsin DPM1 med slavar eller extra konfigurerings- och diagnosstationer. Ingångs- och utgångsinformation kan läsas av alla mastrarna, men endast en master (den som tilldelats slaven under konfigureringen) kan ha skrivaccess.

Diagnostikfunktioner

Diagnostikfunktionerna hjälper till att lokalisera fel snabbt. Diagnosmeddelanden överförs på bussen och samlas in av mastern. Diagnosmeddelanden delas in i tre nivåer, stationsspecifik diagnostik, modulrelaterad diagnostik och kanalrelaterad diagnostik.

Diagnosmeddelandena stationsspecifik diagnostik meddelar allmänt hur en station fungerar. Det kan vara meddelanden om överbelastning, för låg matningsspänning eller interface ej klart.

Diagnosmeddelandena modulrelaterad diagnostik indikerar att fel finns i en specifik I/O modul i en station.

Diagnosmeddelandena kanalrelaterad diagnostik visar att ett fel är relaterat till en individuell in/utgångsbit (kanal), exempelvis en kortsluten utgång.

Systemstatus

Profibus har för att garantera en hög grad av utbytbarhet av produkter av samma typ standardiserat systemegenskaperna för DP. Systemstatus för DP bestäms huvudsakligen av driftstatus hos DPM1. Driftläget kontrolleras antingen lokalt eller över bussen från konfigureringsenheten. Det finns tre olika driftlägen:

- *Stop*, inget datautbyte mellan DPM1 och slavarna
- *Clear*, DPM1 läser ingångsinformation från slavarna och håller utgångarna i ett felsäkert läge
- *Operate*, DPM1 i dataöverföringsläge. Ingångarna läses från slavarna och utgångarna skickas till slavarna cykliskt kontinuerligt.

DPM1 sänder med ett visst tidsintervall (konfigurerbart) sin status till alla sina tilldelade slavar i form av ett multicastmeddelande.

Cyklisk datakommunikation

Datakommunikation mellan DPM1 och dess tilldelade slavar sköts automatiskt av DPM1 i en definierad upprepad sekvens. Användaren gör slavtilldelningen i konfigurationen av bussystemet och bestämmer vilka slavar som inkluderas/exkluderas i den cykliska datakommunikationen. Datakommunikationen mellan DPM1 och slavarna är indelad i tre faser, parametrering, konfigurering och dataöverföring. Innan en slav inkluderas i

dataöverföringen kontrolleras under parametrerings- och konfigureringsfaserna att enhetens konfigurerade data stämmer med slavens verkliga konfigurering. Vid denna kontroll måste slavens typ, ID-nummer, såväl som format, längd och antal för ingångar och utgångar stämma. Detta ger ett pålitligt skydd mot parametreringsfel.

Sync och freeze mod

Mastern kan sända kommandon till alla slavar eller till en grupp av slavar. Dessa styrkommandon skickas som multicastmeddelanden och aktiverar sync och freeze mod för händelsestyrd synkronisering av slavarna. Slavarna börjar sync mod när de får ett sync kommando från sin master. Utgångarna hos alla berörda slavar fryses då vid dess aktuella status. Under följande dataöverföring sparas utgångsdata hos slavarna och utgångarna behåller samma värden. De sparade utgångsvärdena sänds till utgångarna först efter att nästa sync kommando mottagits. Sync mod avslutas med kommandot ”unsync”.

Freeze mod uppstår när en slav mottar ett freeze kommando från sin master. Ingångarna hos alla berörda slavar fryses då vid dess aktuella värden. Ingångsdata uppdateras inte förrän att slaven mottagit nästa freeze kommando. Freeze mod avslutas med kommandot "unfreeze".

Säkerhet

För att skydda dataöverföringar har DP säkerhetsfunktioner mot felaktig parametrering och fel hos överföringsutrustningen.

DPM1 använder en Data-Control-Timer för att övervaka datakommunikationen med slavarna. En separat timer används för varje slav. Timern larmar så fort korrekt dataöverföring inte kunnat utföras inom den konfigurerade övervakningstiden. När så sker meddelas användaren.

Slavarna använder sig av en watchdogkontroll för att upptäcka fel hos mastern eller överföringen. Om ingen datakommunikation sker från mastern inom övervakningstiden sätter slaven automatiskt utgångarna till felsäkert läge. Slavarna har även en annan skyddsfunktion, accesskyddet. Accesskyddet ser till så att bara den auktoriserade mastern har direkt access till slaven ifråga. Till de andra mastrarna tillhandahåller slavarna en avbildning av sina ingångar och utgångar som kan läsas utan accessrättigheter.

DP-V1

DP-V1 har utökade funktioner för acyklisk datakommunikation, vilket är en förutsättning för parametrering respektive kalibrering av fältenheter under drift, för användning av larm och kvittering av larm. Överföring av acykliska data utförs parallellt med den cykliska datakommunikationen, fast med lägre prioritet.

Diagnostik

I DP-V1 har den stationsspecifika diagnostiken utökats och delats upp i larm och statusmeddelanden.

DP-V2

DP-V2 tillhandahåller en funktion för direkt och därmed snabb kommunikation mellan slavar. Kommunikationen sker genom Broadcast utan behov att gå via en master. Slaven är publicerare av Broadcastmeddelandet. I den ordinarie cykliska uppdateringen svarar slaven med sina ingångsdata i form av ett Broadcastmeddelande istället för ett riktat till mastern. Andra slavar kan därmed läsa data direkt från sändande slav och använda dem som egna ingångar, vilket öppnar möjligheter för nya applikationer. Svarstiden på bussen reduceras med upp till 90 %.

Isosynkron mod

Denna funktion ger klocksynkron styrning/reglering av master och slavar, oberoende av busslasten. Funktionen möjliggör mycket precis positioneringsreglering över bussen med ett tidsfel på mindre än en mikrosekund. Alla slavars interna cykler är synkroniserade med masterns cykel genom ett "global control" Broadcastmeddelande. Synkroniseringen kan övervakas genom ett speciellt livstecken.

Klocksynkronisering

Denna funktion synkroniserar alla stationerna till en systemklocka med en avvikelse på maximalt en millisekund, genom att en realtidsmaster sänder tidmärkning till alla slavar över en ny icke fast förbindelse kallad MS3 service, därmed kan händelser tidmärkas exakt. Detta är speciellt användbart för registrering av tidsberoende funktioner i ett nätverk med mer än en aktiv master. Därmed klaras såväl tidmärkning av larm och händelser som planering av tidpunkten för framtida händelser.

Uppladdning och nedladdning

Denna funktion gör att man kan ladda ned/upp en dataarea av valfri storlek till/från en fältenhet med ett enda kommando. Därmed kan program uppdateras och enheter bytas utan att man manuellt måste sköta nedladdningen. Genom att man anger längd i ett läs-/skrivuppdrag är det också möjligt att accessa bara en del av ett datablock. Efter en lyckad access av ett datablock sänder slaven ett positivt svar och om något problem uppstår sänder slaven ett svar som indikerar vilket fel som uppstått.

Adressering i DP

När Profibus adresserar data förutsätts att den fysiska strukturen hos slavarna är modulär eller kan struktureras internt i logiska funktionsenheter, så kallade moduler. Dessa moduler används även i basfunktionerna för cyklisk datakommunikation, där varje modul har ett konstant antal in- och utgångsbyte som överförs på en bestämd plats i datameddelandet. Adresseringsproceduren baseras på identifikationsnummer, som karakteriserar en modultyp som ingång, utgång eller en kombination av båda. Alla identifikationsnumren tillsammans ger konfigurationen för slaven, vilket också kontrolleras av DPM1 vid uppstart av systemet. De acykliska tjänsterna baseras även de på samma modell. Alla datablock som förses med läs/skriv access räknas också till modulerna och kan adresseras genom att man anger slotnummer och index. Slotnumret adresserar modulen och index adresserar datablocken som tilldelats modulen. Varje block kan ha upp till 244 byte. För modulära stationer knyts

slotnumren till modulerna. Modulerna får slotnummer 1 och uppåt i jämn följd. Slotnummer 0 är för stationen själv. Kompaktenheter betraktas som en enhet med virtuella moduler. Dessa kan också adresseras med slotnummer och index.

22.3.6 Profiler

Det finns två typer av applikationsprofiler, allmänna och speciella. Allmänna applikationsprofiler beskriver de funktioner och egenskaper som relaterar till alla applikationer. Speciella applikationsprofiler löser nyckelbehov för användarna i ett flertal industribranscher. De två olika sorternas applikationsprofiler kan användas tillsammans.

Systemprofiler är en behövlig motpart till applikationsprofiler, de specificerar systemegenskaperna som fältenheterna kan använda sig av. Applikationsprofilerna har krav på vissa systemegenskaper för att de ska kunna implementera önskade funktioner. Profibus arbetar på att ta fram en rad systemprofiler baserade på beprövade applikationer i fält. Dessa förväntas samlas i specifikationer inom kort och utökas med ytterligare profiler för att klara framtida krav. De olika typerna av applikationsprofiler beskrivs nedan.

Bara produkter och system med samma profil ger interoperabilitet i en buss respektive ett nätverk.

Allmänna applikationsprofiler

Det finns fyra stycken allmänna applikationsprofiler, PROFIsafe, HART, Tidmärkning och Slavredundans. De beskrivs nedan.

PROFIsafe

PROFIsafe definierar hur felsäkra enheter (nödstoppsknappar, ljusridåer, överfyllnadsskydd med mera) kan kommunicera över Profibus med felsäkra kontroller så säkert att de kan användas för säkerhetsrelaterad automation upp till KAT4 (enligt EN954), AK6 eller SIL3 (Safety Integrity Level). Det innebär säker kommunikation enligt en profil som föreskriver ett speciellt format för användardata och speciella övervakningsfunktioner till protokollet utan att inverka på befintlig PROFIBUS kommunikation.

Specifikationen har tagits fram i samarbete mellan leverantörer, användare, standardiseringskommittéer och institutioner (TÜV, BIA). Den är baserad på befintliga standarder, i första hand IEC 61508, som speciellt behandlar mjukvaruutveckling.

PROFIsafe tar hänsyn till många olika fel som kan uppstå vid seriell busskommunikation, som till exempel fördröjning, förlust eller upprepning av data, felaktig telegramordning, feladressering eller korrupta data.
Det har vidtagits en rad åtgärder för riskreducering i PROFIsafe:

- Numrering i stigande serie av alla säkerhetstelegram
- Tidsövervakning (timeout) för inkommande telegram och deras kvittering
- Identitetskontroll av sändare och mottagare (”password”)

- Extra datasäkerhet (Cyclic Redundancy Check, CRC)

Hart

I dagens industri finns ett stort antal HART-produkter installerade. Med anledning av detta har Profibus i samarbete med HART foundation tagit fram en specifikation som garanterar fullständig konformitet med HART-specifikationerna.

Denna specifikation definierar en applikationsprofil för PROFIBUS som implementeras i masters och slavar ovanför OSI-modellens skikt 7. Den innebär att HARTs client-master-server-modell mappas på Profibus.

Tidmärkning

För att registrera tidsförloppet i ett nätverk, vilket är viktigt vid bland annat diagnostik och felsökning, tillhandahålls en tidsmärkningsprofil i Profibus. Förutsättningen för att kunna göra detta är en klockfunktion hos slavarna som synkroniseras. I Profibus görs detta med hjälp av MS3. En händelse kan få en exakt systemtidsmärkning och på samma sätt kan en tidmärkning avläsas.

Ett koncept av olika prioriterade meddelanden används. Meddelandetyperna sammanfattas med begreppet *”Alerts”* och är uppdelade i högprioriterade ”larm” (dessa överför ett diagnostikmeddelande) och lågprioriterade ”händelser”. I båda fallen, läser masterna cykliskt de tidstämplade processvärdena och larmen från larm- och händelsebufferten hos slaven

Slavredundans

Fördelarna med redundanta slavenheter är att de ger hög tillgänglighet, korta omställningstider, ingen dataförlust och ökar feltoleransen. Den slavredundanta mekanismen hos Profibus har följande egenskaper:

- Slavenheter kan ha två olika Profibus gränssnitt som kallas primary och backup. Dessa kan antingen finnas i en och samma station eller fördelat på två stationer.
- Enheterna är försedda med två oberoende protokollstackar med en speciell redundant utökning.
- Den redundanta kommunikationen löper mellan de två protokollstackarna i samma enhet eller mellan de två separata enheterna, helt oberoende av PROFIBUS och effektiviteten bestäms till största delen av redundansomställningstiden.

I normal drift sker kommunikationen helt över den primära slaven och bara den är konfigurerad. Diagnostikdata från backupslaven skickas av den primära slaven till mastern. I de fall den primära slaven inte fungerar tar backupslaven över dess funktioner, antingen för att den själv har upptäckt felet eller för att mastern begär det. Mastern övervakar alla slavarna och sätter ett diagnostikmeddelande så snart backupslaven inte fungerar eller det inte finns någon redundans. En redundant slavenhet kan operera på en enkel Profibus lina eller, om det finns ett redundant Profibusnät, på två linor.

Speciella applikationsprofiler

De speciella applikationsprofiler som finns eller är under utveckling finns redovisade i tabell 12. I dagsläget finns det ingen speciell applikationsprofil anpassad för trafikstyrning.

Profil	***Profilinnehåll***
PROFIdrive	*Profilen specificerar egenskaperna och accessproceduren för data till hastighetsreglerade elektriska drivutrustningar på Profibus.*
PA devices	*Profilen specificerar karakteristika för processenheter på Profibus inom processautomation.*
Robots/NC	*Profilen beskriver hur hanterings- och sammansättningsrobotar kan styras över Profibus.*
Panel devices	*Profilen beskriver hur enkla human machine interface enheter (HMI) ansluts med Profibus till andra automationssystem.*
Encoders	*Profilen beskriver interfacet till Profibus för roterande vinkel- och linjära enkodrar med envarvs- eller flervarsupplösning.*
Fluid power	*Profilen beskriver styrningen av hydrauliska drivutrustningar över Profibus. Framtagen i samarbete med VDMA.*
SEMI	*Profilen beskriver karakteristika för enheter inom halvledartillverkningen för anslutning till Profibus (SEMI standard)*
Low-voltage switchgear	*Profilen definierar datautbytet med lågspänningsenheter (omkopplare, motorstarter med mera) på Profibus DP.*
Dosage/weighing	*Profilen beskriver implementeringen av våg- och doseringssystem på Profibus DP.*
Ident systems	*Profilen beskriver kommunikationen mellan enheter för identifikationsändamål (streckkoder, transpondrar).*
Liquid pumps	*Profilen definierar implementeringen av vätskepumpar på Profibus DP. Framtagen i samarbete med VDMA.*
Remote I/O for PA devices	*På grund av deras speciella plats i busshanteringen gäller en annan enhetsmodell och andra datatyper för decentraliserade I/O på Profibus PA jämfört med instrument och dylika.*

Tabell 12 Profibus special applikationsprofiler (Källa: Profibus Teknologi och användning med vissa förändringar)

22.3.7 PROFInet

PROFInets kommunikationsmodell definierar en tillverkaroberoende standard för kommunikation på Ethernet med standard IT-mekanismer. PROFInet använder sig av TCP/IP och COM/DCOM. Vilket ger direkt access från kontorsvärlden genom hela automationshierarkin och omvänt (vertikal integration).

Kommunikation

PROFInets Ethernetbaserade kommunikation kan delas i tre prestandanivåer.

1. TCIP/UDP och IP för icke-tids-kritiska data.
2. Soft Real Time (SRT) för tidskritisk process data använd på fältet i industriautomation.
3. Isochronous Real Time (IRT) för särskilt sofistikerade krav.

Dessa tre prestandanivåer av kommunikation täcker hela spektrat av automationsapplikationer.

Kommunikation med TCP/UDP

PROFInet använder Ethernet och TCP/UDP tillsammans med IP som bas i sin kommunikation. Då PROFInet inte specificerar vilka protokoll som ska användas över TCP/UDP (skikt 4 i OSI-modellen) så är interoperabilitet endast garanterad om samma överliggande protokoll används.

SRT

SRT är en optimerad realtidskommunikationskanal. Kanalen är Ethernet baserad och således berör den bara skikt 1 och 2 i OSI-modellen. Denna lösning gör att körtiden i kommunikationsstacken minimeras och prestationen ökar med avseende på uppdateringshastighet på processdata. Detta görs genom eliminering av protokoll i de övre skikten. Vilket reducerar meddelande längden och minskar tiden för att överföringsdata ska vara redo att sändas respektive redo för att bearbetas av processorn. Samtidigt minskar behovet för processorkraft hos i utrustningen för kommunikation.

Överföringen i nätverket är även den optimerad genom att datapaketen är prioriterade enligt standarden IEEE 802.1Q. Innebörden av detta är att dataflödet mellan utrustningar är kontrollerat av nätverkskomponenter med hänsyn till de olika prioriteringsklasserna. Prioritet 6 är standard prioriteten för realtidsdata, detta gör att realtidsdata prioriteras före exempelvis Internet telefoni som har prioritet 5.

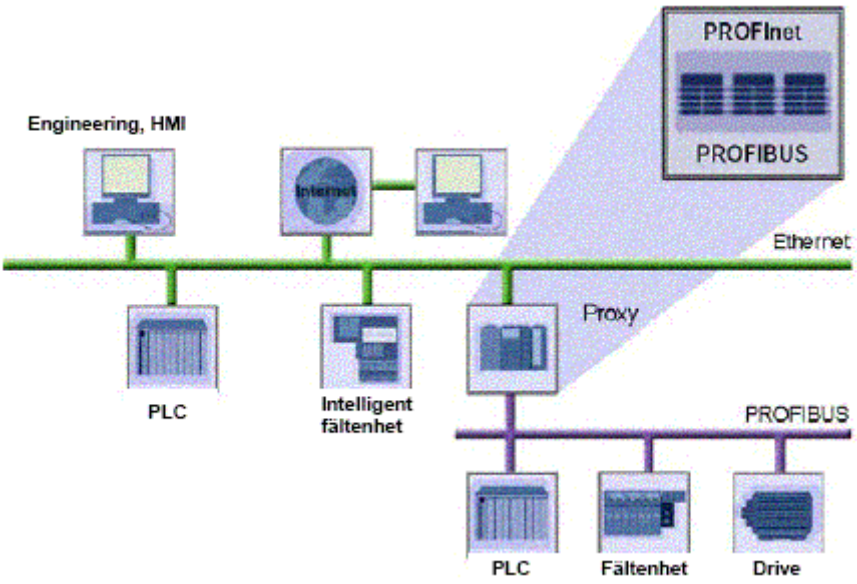
IRT

Lösningen för SRT är inte tillräcklig för rörelsekontroll som har krav på uppdateringsintervall på omkring 1 ms med ett maximalt jitter på 1 µs. För att mötta dessa krav har PROFInet definierat en tids-lucka-kontrollerad (time-slot-controlled) överföringsmetod kallad IRT som ett skikt 2 (i OSI-modellen) protokoll för Fast Ethernet.

Genom tidsynkronisering mellan deltagande utrustningar kan en tidslucka definieras i nätverket för överföringen av viktiga data. Kommunikationscykeln är delad i en deterministisk del och en öppen del. Där de cykliska realtidspaketen är överförda i den deterministiska kanalen och TCP/IP paketen i den öppna kanalen.

22.3.8 Migration

Migration kan ske mellan PROFInet och Profibus med hjälp av en proxy. I figur 13 ses en figur över hur det kan se ut. Proxyteknologin tillåter också att andra fältbussystem inkluderas.



Figur 13 Migration mellan Profibus och PROFInet (Källa: Profibus Teknologi och användning)

22.3.9 Databeskrivning

För databeskrivningen används XML.

22.3.10 Certificering

För att Profibus produkter framtagna av olika leverantörer ska kunna fungera felfritt krävs att implementeringen av kommunikationsprotokoll och applikationsprofiler gjorts i enlighet med standard. För att garantera detta utfärdar Profibus organisationen certifikat för de produkter som klarat ett test för detta ändamål.

22.3.11 Tillgänglighet

Det finns olika typer av medlemskap med skilda kostnader (från 1200 kr till 30 000 kr per år) beroende på företagsstorlek och intresse.

22.3.12 Användning

Profibus används främst inom ITS för styrning av variabla skyltar, bland annat används Profibus i MTM-systemet i Stockholm.

23 Bilaga 3

Nedan beskrivs världsstandarder med ITS-anknytning, dessa standarder täcker med skild grad berörda ITS-områden. Informationen om standarderna har inhämtas från respektive standards bakomliggande organisation, på grund av detta är informationen mer eller mindre partisk och brister kan ha undanhållits.

23.1 IVERA

IVERA är ett holländskt protokoll som tagits fram för att tillhandahålla en tillverkaroberoende lösning för kommunikation mellan kontrollcentraler och trafiksignaler. Protokollet kan även användas i andra kommunikationssystem. Namnet IVERA är en kombination av förkortningarna för Initiatiefgroep VErkeersregeltechnici Rijkswaterstaat en Provincies (IVER, Initiative Group of Traffic Control Engineers of Department of Public Works and Provinces) och ASsociation of TRaffic Industries in the Netherlands (ASTIN) som är två av de bakomliggande organisationerna.

23.1.1 Omfattning

Initialt har IVERA protokollet blivit utvecklat för kommunikation mellan trafiksignaler och en kontrollcentral. I tillägg till det passar IVERA protokollet för applikationer som:

- Kommunikation med system för påfartskontroll
- Kontroll av skyltar i parkeringssystem
- För sammanlänkning av kontrollcentraler

I designen av IVERA protokollet är utgångspunkten ett maximalt användande av standard kommunikationsinrättningar för både kommunikationsinfrastruktur och –mjukvara. Fördelar med detta är:

- Stöd av olika kommunikationsnätverk som telefonnätet och punkt till punkt kabel kommunikationer
- Stöd av befintliga protokoll
- Tillverkaroberoende lösningar
- Minimal utvecklingsansträngning genom användande av standard hårdvaru- och mjukvarukomponenter

23.1.2 Medverkande

Initiativtagare till IVERA protokollet är ASTIN, Commissie Verkeersregeltechnici Nederland (CVN, Committee of Traffic Control Engineers in The Netherlands) och IVER.

ASTIN är en organisation för holländska bolag som arbetar med trafikteknik. Medlemmar är Peek Traffic, Siemens Nederland, TPA Traffic and Parking Automation och Vialis Verkeer en

Mobiliteit. CVN är en kommitté för trafiksignalingenjörer i Holland. IVER är en sammanslutning bestående av Hollands fyra största städer.

En arbetsgrupp bestående av delegater från IVER och ASTRIN är ansvariga för genomförandet av IVERA. Arbetsgruppens uppgift är ett skriva en funktionell specifikation för kommunikation mellan ett centralt system och trafiksignaler.

Protokollet ägs av stiftelsen Beheer ASTRIN/IVERA protocol.

23.1.3 Kommunikationsmodell

IVERA protokollet tillhör skikt 7 i OSI-modellen. IVERA protokollet kommunicerar med underliggande nätverksskikt via standardfunktioner (stream eller fil I/O). IVERA protokollet gör följande antaganden med avseende på underliggande skikt:

- Underliggande skikt tillhandahåller skapande och underhåll av en förbindelseorienterad förbindelse mellan IVERA master och IVERA slav. En möjlig implementering för en sådan förbindelse är en förbindelse baserad på TCP/IP.
- Underliggande skikt säkerställer att de byte som skickas av IVERA mastern anländer felfritt och i samma ordning till IVERA slaven och vice versa.
- Underliggande skikt tillhandahåller segmentering och routing.
- I de fall när mer än en logisk förbindelse finns mellan kontrollcentral och trafiksignaler över samma fysiska förbindelse har IVERA meddelanden prioritet.
- Om datakomprimering krävs eller är nödvändig så ska den implementeras i lägre skikt.
- Om datakryptering krävs ska den implementeras i lägre skikt.

IVERA protokollet fungerar över TCP/IP och PPP, för vilket lösningar kan certifieras hos stiftelsen Beheer ASTRIN/IVERA protocol. Eventuellt kommer det även att fungera direkt över en fysikförbindelse.

Logik

IVERA protokollet är ett master/slav protokoll. Via IVERA protokollet kan en master läsa objekt från och skriva objekt till en slav. Normalt är kontrollcentralerna master och trafiksignalerna slavar. I IVERA kan både master och slav ta initiativ till att inrätta en förbindelse. När förbindelsen är upprättad är protokollet operativt. Mastern får information från slaven genom att läsa objekt, mastern ändrar en parameter genom att skriva ett nytt värde i motsvarande objekt. För att få slaven att utföra ett kommando skriver mastern ett nytt värde till ett speciellt objekt i slaven. Hos slaven finns definitioner för vad slaven ska göra beroende på vilket kommando den fått lagrade.

Objekt

I IVERA definieras ett objekt enligt följande:

- Ett objekt är något som kan bli valt och manipulerat som en enhet
- För att ett objekt ska kunna väljas har varje objekt ett unikt namn

- Alla data från ett objekt är av samma typ

För varje typ av implementering (exempelvis kommunikation mellan kontrollcentraler) finns en unik uppsättning av objekt definierade. Namngivande till dessa objekt görs med hjälp av en speciell namngivningskonvention. Målsättningen är att standardisera så många objekt som är möjligt för en implementering.

I en IVERA slav består ett objekt av följande:
- Unikt objektnamn
- Objektattribut
- Dataelement

Objektattributen innehåller alla kännetecken för objektet. Dataelementen innehåller den data som är sparad i objektet. Dataelementen är sparade som en eller flerdimensionerade arrayer. För varje objekt är antalet dimensioner och antalet dataelement per dimension justerbara. Av praktiska själ är antalet dimensioner per objekt begränsade till tre. Maximala antalet dataelement per objekt är 2^{16} (65636). För varje dataelement finns möjligheten att definiera ett dataformat.

I IVERA finns ett förenklat sätt att se de olika objekten på, där objekten delas in i fyra huvudområden, basobjekt, indexobjekt, kommandoobjekt och händelseobjekt. Ett basobjekt innehåller en lista med namn på alla objekt av en specifik typ som finns hos en slav. Antalet dataelement hos ett basobjekt korresponderar med antalet objekt av en specifik typ. I ett indexobjekt innehåller dataelementen de logiska namnen för dataelementen i ett annat objekt. Kommandon skickas från mastern till slaven via kommandoobjekt. Att sända ett kommando är implementerat på samma sätt som skriva ett värde till ett dataelement i ett objekt. Kombinationen av objekt, dataelement och värde bestämmer vilket kommando som är gett.

Händelser är något som händer i en slav. Dessa händelser sparas av slaven i ett händelseobjekt. Mastern kan få veta vilka händelser som har skett genom att läsa det associerade objektet. Efter att mastern har läst om en händelse kan den konfirmera att den har gjort det. Ett händelseobjekt karakteriseras av att antalet dataelement inte är konstant. Antalet element korresponderar med antalet händelser i händelseobjektet.

Flera implementeringar kan ha objekt med samma namn där funktionaliteten kan vara olika beroende på applikation. Detta skapande av homonymer är inget problem då varje objekt har en unik implementeringsidentifikation (TID) som kan läsas från slaven med hjälp av protokollet.

I IVERA är datainnehållet standardiserat så att vissa basfunktioner säkerställs. Utöver dessa basfunktioner finns möjligheter till att definiera apparatspecifika och applikationsspecifika funktioner

23.1.4 Säkerhet

I IVERA är en användare något eller någon som kan tillträda en slavs objekt via IVERA protokollet. För att hålla systemet så enkelt som möjligt har inte en slav individuella användare utan enbart användargrupper. En användargrupp är en samling av användare med

samma rättigheter. En IVERA slav stödjer fyra användargrupper, där rättigheterna kan sättas för varje objekt.

Varje användargrupp har sitt eget lösenord. Inloggning går till så att mastern skriver till objektet ”LOGIN”. Lösenorden fastställs endast en gång och kan inte modifieras. Efter tre misslyckade login försök avbryts kommunikationsförbindelsen av slaven. Endast objekten ”LOGIN” och ”PING” kan läsas och skrivas utan en lyckad inloggning. ”PING” objektet används för synkronisering mellan mastern och slaven.

Utloggning är möjlig att göra på tre sätt:

- Genom att avbryta förbindelsen mellan mastern och slaven
- Genom en timeout på en halv timme, där det inte är någon aktivitet från mastern
- Genom ett kommando

I objekten finns ett attribut som heter User Identification Control (UIC). UIC attributet är en mask som indikerar vilka rättigheter en användargrupp har till access av ett objekts dataelement. Klassifikationen av UIC: s mask korresponderar till användarrättigheterna i UNIX. Där det finns åtta nivåer av användarrättigheter avhängiga på rätten till att skriva, läsa och exekvera. Då IVERA protokollet endast stödjer läsa och skriva så finns det tre olika nivåer av användarrättigheter:

1. Inga rättigheter alls
2. Endast läsrättigheter
3. Läs- och skrivrättigheter

Loggbok

För varje objekt måste det fastställas om ändringar i dataelementen ska sparas i en parameterloggbok.

Övriga säkerhetsfunktioner

Övriga säkerhetsfunktioner får implementeras i lägre skikt.

23.1.5 Master/slav synkronisering

Det finns ett ”PING” objekt i alla slavar. Detta objekt har ingen betydelse för slaven, men kan användas av mastern för att synkronisera mastern och slaven. För att synkronisera mastern och slaven skriver mastern ett slumptal i ”PING” objektet. ”PING” objektet ger även möjlighet till att mäta tiden som ett meddelande är på väg från mastern till slaven och tillbaka till mastern.

Meddelandenummer

Vid kommunikationen mellan två datorer, exempelvis kommunikation mellan kontrollcentral och styrapparat, används meddelandenummer. Mastern genererar meddelandenumren, slaven skickar tillbaka meddelandenumret när den fått det. Mastern jämför svaret från slaven med det första meddelandet i överföringsbufferten. Om meddelandenumren matchar skickas svaret till applikationen. I fall där meddelandenumren inte matchar ignoreras svaret och mastern resynkroniserar förbindelsen. Om slaven svarar med felmeddelandet ”ERR_ILLEGAL” har slaven mottagit ett ogiltigt meddelande, förbindelsen resynkroniseras då av mastern. Om slaven svarar med ett annat felmeddelande än ”ERR_ILLEGAL”, återkallas meddelandet från överföringsbufferten och en felkod skickas till applikationen.

I fall när meddelanden är inlagda manuellt finns ingen nytta av meddelande nummer.

Timeout

I exceptionella fall kan det ske att mastern inte får något svar, fast de underliggande nätverksskikten indikerar att förbindelsen mellan mastern och slaven är i ordning. För att upptäcka denna situation har mastern en timeout timer. När timeout tiden gått ut resynkroniserar mastern förbindelsen.

Bruten förbindelse

Om förbindelsen mellan mastern och slaven misslyckas/bryts rapporteras detta till IVERA protokollet från de underliggande nätverksskikten. IVERA avbryter då alla aktiviteter som är under bearbetning. Med detta menas att mastern inte sänder fler meddelanden förrän förbindelsen är återskapad och att slaven slutar skicka eventuella svarsmeddelanden.

23.1.6 Händelser hos slaven

När en händelse sker hos en slav tar slaven initiativ till att inrätta en förbindelse. När förbindelsen är upprättad skickar slaven ett händelsemeddelande (BerichtSlaveTrigger) till mastern. Ett händelsemeddelande som skickats automatiskt från slaven till mastern innehåller ingen händelseinformation utan väcker enbart mastern så att den vet att en händelse skett. Efter att mastern mottagit händelsemeddelandet är det masterns uppgift att läsa information från slaven för att ta reda på vad som hänt.

23.1.7 Övrigt

I IVERA finns en ändringsräknare (valfritt tillval). Ändringsräknaren är kopplad till ett objekt, när ett dataelement i ett objekt ändras ökar en variabel. Denna flagga är passande för objekt med ett stort antal dataelement som ändras sporadiskt. Ändringsräknaren gör så att en master som är intresserad av ändringar inte behöver läsa alla dataelement regelbundet.

23.1.8 Användning

IVERA protokollet används i Holland av företagen Peek Traffic, Siemens Nederland, TPA Trafic en Parking Automation, Vialis Verkeer en Mobiliteit och Ko Hartog. I dagsläget finns protokollet installerat i ca 400 trafikledningsinstallationer, antalet växer kontinuerligt.

23.1.9 Tillgänglighet

För användning av IVERA protokollet utfärdar stiftelsen ”Beheer ASTRIN/IVERA protocol” licenser.

23.2 National Transportation Communications for ITS Protocol (NTCIP)

National Transportation Communications for ITS Protocol (NTCIP) är en familj av standarder för överföring av data och meddelanden mellan kontrollsystem och apparater använda inom ITS. Det är baserat på datakommunikationsstandarder.

23.2.1 Omfattning

NTCIP: s standarder är tänkta att kunna användas i alla sorters ledningssystem som hanterar något inom trafikmiljön, exempelvis de för motorvägar, trafiksignaler, räddningsledning, transittrafik, resandeinformation och dataarkivering. Det är tänkt att användas för fast och trådlös kommunikation mellan datorer i olika system eller ledningscentraler och datorer eller apparater efter vägar.

NTCIP omfattar ej standarder för:

- Kommunikation mellan fältapparater och fordon. Kommunikation mellan fältapparater och centraler stöds.
- Överföring av videobilder i full upplösning. Överföring av videokamerans kontrolldata och ändringskontrolldata stöds genom användning av en separat kommunikationskanal.
- Överföring av resandeinformation till privat ägda fordon. Här inkluderas speciella Broadcasting och begränsade bandbredds protokoll som arbetar i samarbete med FM radiostandarder och mobilradio. Överföring av information från olika källor till resandeinformationscentralen stöds.
- Kommunikation för finansiella transaktioner
- Fordonsintern kommunikation för exempelvis avancerad fordonskontroll och säkerhet.
- Kommunikation mellan styrapparat och annan elektronisk utrustning i RSC-skåp.

23.2.2 Medverkande i NTCIP

För att säkerställa både leverantörers, användare och regeringens (USA:s regering) stöd, så är NTCIP ett samarbete mellan National Electronics Manufacturers Association (NEMA), American Association of State Highway and Transportation Officials (AASHTO) och Institute of Transportation Engineers (ITE) med ekonomiskt stöd från Federal Highway Administration (FHWA). De olika organisationerna har inga speciella roller i NTCIP utan arbetet styrs av en kommitté, där de tre organisationerna har sex medlemmar vardera.

23.2.3 Protokoll i NTCIP

NTCIP tillhandahåller standarder för två olika typer av ITS kommunikationer. Den första typen är kommunikation mellan ledningssystem eller centraler och multipla kontroll- eller övervakningsutrustningar som styrs av systemet eller centralen. Då de flesta av dessa system involverar en dator eller ett ledningssystem som kommunicerar med olika typer av apparater efter vägkanter och verksamhetsfordon kallas denna typ av kommunikation för ”center-to-field” (C2F, central-till-fält). Exempel på C2F system är variabla skyltar, trafiksignaler, fordonsdetektorer och vädersensorer.

Den andra typen är kommunikation mellan centrala ledningssystem. Denna typ av kommunikation kallas ”center-to-center” (C2C, central-till-central). Exempel på C2C system är trafikledningssystem, parkeringsledningssystem, olycksledningssystem och reseinformation.

Bägge dessa kommunikationstyper har en delvis gemensam kommunikationsmodell med protokoll som beskrivs nedan.

23.2.4 Kommunikationsmodell

NTCIP använder sig av en skiktmodell som liknar OSI-modellen. Istället för OSI-modellens sju skikt innehåller NTCIP: s modell fem skikt, informationsskiktet, applikationsskiktet, transportskiktet, subnätverksskiktet och anläggningsskiktet.

Informationsskiktets standarder definierar innebörden av data och meddelanden och den generella hanteringen av ITS information. Skiktet är ovanför OSI-modellens högsta skikt och således saknas motsvarande skikt i OSI-modellen.

Applikationsskiktets standarder definierar regler och procedurer för överföring av informationsdata. Det motsvaras i stort av applikations-, presentations- och sessionskiktet i OSI-modellen.

Transportskiktets standarder definierar regler och procedurer för överföring av applikations data från punkt ”X” till punkt ”Y” i ett nätverk, inkluderat är routing, meddelande hopsättning/isärtagning och nätverksmanagement funktioner. I OSI-modellen motsvaras det i stort av transport- och nätverksskiktet.

Subnätverksskiktets standarder definierar regler och procedurer för överföring av data mellan två ”intilliggande” apparater över något kommunikationsmedium. Det motsvaras i stort av datalänk- och fysiska skiktet i OSI-modellen.

I anläggningsskiktet bestäms vilken kommunikationsinfrastruktur som används för kommunikationen. Att notera är att anläggningsskiktet inte är ett val av standard utan ett val av infrastruktur, vilket påverkar valet av standard i subnätverksskiktet. Motsvarande skiktet saknas i OSI-modellen.

<table>
<tr><th>OSI-modellen</th><th>NTCIP-modellen</th></tr>
<tr><td></td><td>Informationsskiktet (1)</td></tr>
<tr><td>Applikationsskiktet (7)</td><td rowspan="3">Applikationsskiktet (2)</td></tr>
<tr><td>Presentationsskiktet (6)</td></tr>
<tr><td>Sessionskiktet (5)</td></tr>
<tr><td>Transportskiktet (4)</td><td rowspan="2">Transportskiktet (3)</td></tr>
<tr><td>Nätverksskiktet (3)</td></tr>
<tr><td>Datalänk skiktet (2)</td><td rowspan="2">Subnätverksskiktet (4)</td></tr>
<tr><td>Fysiska skiktet (1)</td></tr>
<tr><td></td><td>Anläggningsskiktet (5)</td></tr>
</table>

Tabell 13 OSI-modellens skikt jämförda med NTCIP-modellens skikt

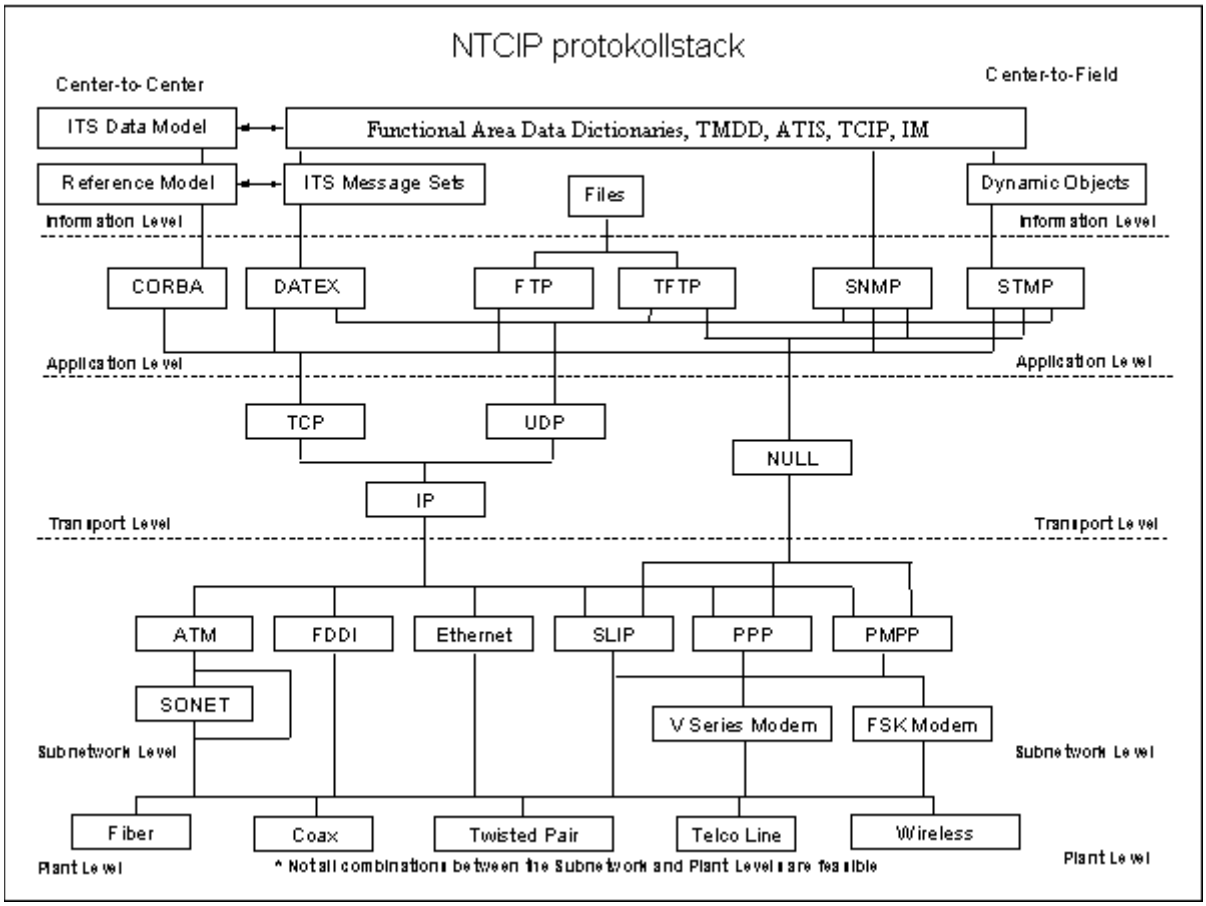
Informationsskiktets standarder som används inom ITS är unika för transportindustrin. Mycket av den pågående standardiseringsansträngningen inom ITS involverar identifikation av obligatoriska dataelement och definition av deras användning för olika domäner och funktioner inom ITS.

På applikations-, transport- och subnätverksskiktet nivå kan ITS i stort sett använda sig av befintliga telekommunikationsstandarder. NTCIP specificerar vilka optioner som ska användas ur en standard när det finns flera alternativ.

NTCIP har utökat befintliga standarder eller utvecklat nya protokoll som behövs i fall där ITS har speciella behov. De två områden där ITS främst har speciella kommunikationskrav är:

- Kontinuerliga, automatiserade, realtidsöverföringar av stora volymer av små datapaket i många-till-många multiförmedlingsnätverk.
- Kontinuerliga höga volymer av realtidsdata skickade till och från processorer vid vägkanter eller fordonsutrustningar som delar samma låghastighetsdatakanal och har krav på låg latens (konstant överföringstids fördröjning).

I NTCIP kan en mängd olika protokoll/standarder användas i respektive skikt. I figur 14 ses en sammanställning över NTCIP: s struktur. Figuren visar de olika protokoll (rutor) som kan användas i respektive skikt och vilka som är kompatibla med varandra (linjer som sammanbinder rutorna). Inte alla kompatibla konfigurationer är användbara fast de är möjliga. Exempelvis så är inte vanligt att använda Simple Network Management Protocol (SNMP), ihop med TCP/IP.



Figur 14 NTCIP: s protokollstack (källa http://www.ntcip.org/library/protocols/ med vissa förändringar)

23.2.5 Anläggningsskiktet

Anläggningsskiktet finns med i NTCIP för att ge en referens för personer som håller på och lär sig om NTCIP. Det bestämmer vilket fysiskt transmissionsmedium som används för kommunikationen, exempel är koppartråd, coaxial kabel, fiberoptisk kabel och trådlös kommunikation.

23.2.6 Subnätverksskiktet

I subnätverksskiktet används en rad standardprotokoll som ATM, ATM/SONET, FDDI, Ethernet, SLIP och PPP. NTCIP har även utvecklat ett eget protokoll Point-to-Multipoint Protocol (PMPP) med bas i standard protokollen PPP och HDLC. PMPP beskrivs nedan.

PMPP

Det primära målet med PMPP standarden är att erbjuda ett enkelt dataöverföringsverktyg som är förbindningslöst. PMPP är tillämparbart för transportrelaterade utrustningar som verkar i primär/sekundär konfigurationer, där en utrustning är betecknas som primär och en eller flera

andra utrustningar agerar som sekundärer och är anslutna till en kanal. En sekundär överför aldrig om det inte tillåtits av primären.

PMPP fungerar på låghastighets kommunikationskanaler som är hel- eller halvduplex. Det används för feldetektering, kontroll och tillkännagivande av länkaktivering och deaktivering.

PMPP hanterar inte organisering och definiering av information relaterad till transportutrustningens slutapplikation. Det kräver inte heller något speciellt transport- eller applikationsprotokoll, men det har Initial Protocol Identifier (IPI) som identifierar högre skikts protokoll. IPI är direkt jämförbar med den protokollidentifiering som används av PPP. Det tillhandahåller en mekanism som tillåter multiplexing av meddelanden genererade av multipla protokoll som använder en fysisk kanal.

23.2.7 Transportskiktet

I transportskiktet används tre olika protokoll, TCP/IP, UDP/IP och Transportation Transport Protocol (T2, tidigare känt som NULL). T2/NULL används när routingbehov saknas. Vid behov av routing skiljs mellan förbindelseorienterade och förbindelselösa uppkopplingar. TCP är förbindelseorienterat och används i symbios med IP som hanterar routingen. UDP är förbindelselöst och även det används i symbios med IP som hanterar routingen.

T2/NULL

T2/NULL tillhandahåller en länkningsmekanism mellan applikations- och nätverksskiktet i icke-nätverksmiljöer. I denna miljö krävs inga andra transport- och nätverksskiktstjänster än övre skikts multiplexering och att transformera gränssnittsinformationen från applikation-transport gränsen till transport-subnätverk gränsen. Det är tänkt att tillhandahålla ett standard gränssnitt som säkerställer interoperabilitet, speciellt i fall där multipla kommunikationstackar samsas.

23.2.8 Applikationsskiktet

I applikationsskiktet skiljs mellan filöverföring, central-till-fält (C2F) och central-till-central (C2C) kommunikation. Respektive typ av kommunikation använder olika protokoll. Nedan beskrivs de var och en för sig.

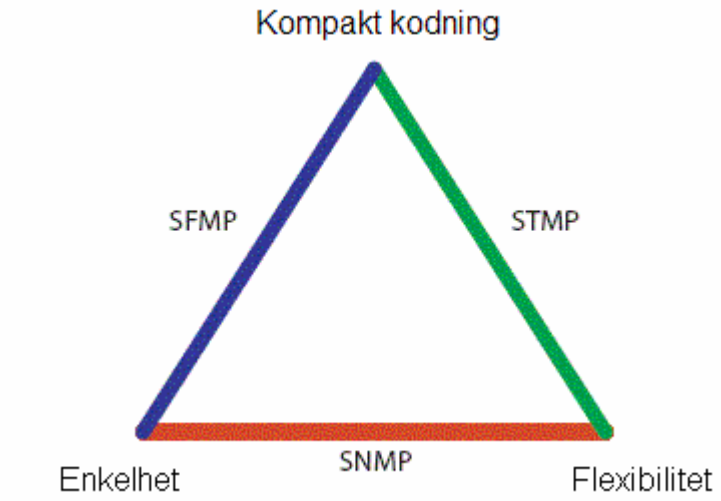
Filöverföring

Som filöverföringsprotokoll används FTP och TFTP.

C2F

För C2F kommunikation används protokollgruppen, Transportation Managemant Protocol (TMP). TMP definierar regler och procedurer för att transportlednings applikationer ska kunna samarbeta med transport utrustningar. TMP är designat för att ha 100 % interoperabilitet med Internetstandarden SNMP, men utökar även SNMPs struktur för att möta behov från transportsektorn. NTCIP: s analyser av transportsektorn har visat att de behov som finns är enkelhet, flexibilitet och minimal datapaketsstorlek.

För att tillgodose dessa krav har NTCIP utvecklat protokollet Simple Transportation Management Protocol (STMP) och håller på att utveckla Simple Fixed Management Protocol (SFMP), bägge har SNMP som bas. Var och ett av de tre protokollen maximerar två av de tre behoven på bekostnad av det tredje, se figur 15 nedan.



Figur 15 (Källa: NTCIP 9001 Exhibit 3.6 med vissa förändringar)

Att SNMP, STMP och SFMP ses som en grupp av protokoll med samlingsnamnet TMP beror på att de använder samma protokollidentifiering. SNMP startar jämt med en identifieringsbyte som är 0x30, det gör att TMP kan använda den första byten till protokollidentifiering. När TMP dekodar en dataström skickas hela bitströmmen inkluderat den första byten till korrekt protokoll. Vid kodning av en dataström skickas bitströmmen som den är till underliggande protokoll. Nedan beskrivs STMP, SFMP och de SNMP egenskaper som är gemensamma. För mer information om SNMP hänvisas till facklitteratur.

SNMP

Alla tre protokollen använder sig av samma få-sätt (get-set) paradigm (tankesystem, böjningsmönster) för överföring av enskilda data delar. Varje datadel sparad i en utrustning är kontaktbar via ett protokoll där den kallas för objekt. Varje objekt består av två delar, ”object type” och ”object instance”.

Varje ”object type” som är sparad i en utrustning är formellt avgränsad i en fil som kallas Management Information Base (MIB). I MIB associeras varje ”object type” med en exakt

syntax, en definition och med en objektidentifierare. Objektidentifieraren är ca 10 byte stor. ”Object instance” identifieras genom att ”instance” nummer läggs till objektidentifieringsnumret. Vilket gör att varje del av data i en utrustning har ett unikt nummer som den associeras med.

SNMP ledningsstationer överför data genom att skicka med objektidentifieringsnummer vid varje få (get) och sätt (set) begäran. Ett meddelande kan innehålla flera begärningar och gör så mestadels. Sålunda innehåller många av alla meddelanden flera av den 10 byte stora objekt identifieringen. I svaren inkluderas objektidentifiering tillsammans med data och i svaren för sätt (set) begärningar inkluderas objektidentifiering.

SNMP är ett enkelt och bandbreddsineffektivt protokoll som passar till nätverk med hög bandbredd eller med en låg volym av meddelanden.

SFMP

SFMP kan ses som en enklare och mer kompakt variant av SNMP. NTCIP har gjort en analys av SNMP som visar att datapaketens storlek och komplexitet kan reduceras genom:

1. Identifiera datainnehållet i ett datapaket genom att använda en identifierare som refererar till en grupp av dataelement istället för att använda enskilda identifierare till varje dataelement i ett datapaket.
2. Definiera en datapaketsstruktur som endast inkluderar den information som krävs för en given meddelandesort.
3. Använda en kodning som är mer effektiv än Abstract Syntax Notation – 1 (ASN.1) Basic Encoding Rules (BER) som används av SNMP.

Data identifiering

SFMP minskar storleken på headern på två sätt. Först är den designad med antagandet att den ska överföra enskilt sammansatta objekt, det vill säga objekt som består av en definierad sekvens av andra objekt. Detta gör att headern minskarpå grund av användning av enskilda objektidentifierare istället för separata identifierare för varje delobjekt. För det andra så infogar SFMPs designkonceptet att sammansatta objekt är lokaliserade under NEMA noden av ISO trädet. Där inkluderas en kodningsmekanism som kortar ner objektidentifierare under denna nod. Protokollets komplexitet är reducerad då en agent inte krävs för att hantera få (get) och sätt (set) kommandon oavsett datakombination och begäran, agent krävs endast för att stödja ett objekt åt gången om objektet är ett block objekt (tillåter att en struktur av dataelement hanteras som ett objekt). Detta gör att mindre komplexitet och kraftfullhet krävs i utrustningarna för att de ska stödja NTCIP.

Paketstruktur

I SNMP använder alla datapaket snarlik datastruktur. Det ger vissa fördelar i kod återbruk, men det resulterar i att extra information överförs i många datapaket. Behovet att minska headern för de mest frekventa överföringarna och för att minska processorkrav för att dekoda dessa extra bytes har NTCIP utvecklat en SFMP datapaketsstruktur som överför fastställda meddelanden effektivare men fortfarande tillhandahålls nödvändiga säkerhetsfunktioner.

Kodning

SNMP kodar all sin information efter ASN.1 BERs regler. BER använder tre ”tuple” för att koda data för överföring. Första tuplen används för att specificera vilken typ av data som följer. Den andra tuplen specificerar hur många oktetter som ockuperas av data. Den tredje tuplen är den aktuella data som ska överföras. Den här typen av kodning kallas för TLV (Type, Length, Value). TLV är en flexibel kodning av information för överföring, men om båda sidor redan har kommit överens om en specifik datastruktur, inkluderas onödig information i headern när datatyp och datalängd finns med när datalängden är fastställd.

På grund av detta har NTCIP definierat Octet Encoding Rules (OER) som är en del av ASN.1 kodningsregler. I OER elimineras datatyps tuplen helt och datalängds tuplen elimineras när datalängden är känd. På grund av att de flesta objektdefinitioner (dataelement) som är definierade av NTCIP består av heltal mellan 0 och 255, kan OER reducera storleken på många NTCIP datapaket.

SFMP är enkelt och bandbredseffektivt.

STMP

STMP är konceptuellt likt SFMP förutom att det är designat för att använda dynamiska objekt. Dynamiska objekt är en grupp av dataelement som definieras under körtid, med andledning av att en kort identifierare ska kunna referera till hela gruppen. Dataelementen är kodade enligt OERs regler.

Dynamiska objekt har fördelen att ledningsstationerna har flexibiliteten att kunna bestämma storleken på sina egna meddelanden. Det negativa är att det ökar komplexiteten hos agentens mjukvara markant.

STMP kräver SNMP eller SFMP för att ledningsstationerna ska kunna sätta värden i dynamiska objekt konfigurationstabellen och i dynamiska objekt definitionstabellen. Dynamiska objekt konfigurationstabellen är en tabell som indikerar vem som äger ett objekt och dess status. Dynamiska objekt definitionstabellen definieras önskat innehåll i det dynamiska objektet.

STMP stödjer 13 dynamiska objekt för varje agent. I teorin kan ledningsstationerna konfigurera varje agent olika, vanligtvis konfigureras lika apparater med samma dynamiska objektdefinitioner. Det låga antalet av olika dynamiska objekt gör att det endast behövs fyra bitar för meddelande identifiering, vilket minskar ner headerns storlek. Inget lösenord krävs heller eftersom de dynamiska objekten definieras i körtid.

STMP använder sig även av ett par av SFMPs förminskningar av headern, för att minska ner datapaketsstorleken jämtemot SNMP.

STMP passar för nätverk med låg bandbredd och en stor volym av meddelanden.

Fällor

Både SNMP och SFMP använder sig av en ”fäll”-mekanism ger agenten möjlighet till att meddela ledningsstationen extraordinära händelser. Exempelvis så kan en ledningsstation vilja veta när en dörr öppnas till ett kontrollrum, så att operatören vet när någon tillträtt rummet. Under TMPs vanliga få-sätt (get-set) paradigmen måste ledningsstationen kontinuerligt tvinga agenten att undersöka om dörrens statusobjekt ändrats. Ledningsstationen kan då missa en ändring i status om statusen ändras så att den är tillbaka i original värde mellan agentens undersökningar.

Fällmekanismen tillåter en agent att meddela ledningsstationen om en extraordinär händelse utan att ledningsstationen framkallat att den ska göra det. Fällor kan även orsaka problem. En av fördelarna med få-sätt (get-set) paradigm är att ledningsstationen har stor del av kontrollen över trafiklasten i kommunikationsnätverket. Introduktionen av fällor gör att ledningsstationerna förlorar en del av sin trafiklastkontroll då agenterna ges möjligheten att överbelasta nätverket med meddelanden om extraordinära händelser. Det översvämmande nätverket kan då hindra ledningsstationen från att åtgärda problemet. På grund av detta motarbetar en del nätverksdesigners användande av fällor.

NTCIP tycker att fällor utgör ett giltigt funktionskrav för systemkommunikation och har därför utvecklat en struktur för hur fällor ska hanteras för att minimera problemen associerade med överbelastade nätverk. Detta görs genom att ledningssystemet ges följande möjligheter:

1. Visar att det känner till fällans meddelande
2. Kontrollera maxantalet fällmeddelande från en apparat
3. Konfigurera apparaten så att den sparar informationen i en loggfil istället för att överföra den som en fälla
4. Hindra fällor tillfälligt

Säkerhet

TMP tillhandahåller säkerhet på basnivå. Huvudsakliga målet är att hindra auktoriserade användare från att komma åt information som de ej är auktoriserade till. Säkerhet mot icke auktoriserade användare ska ske i skikt på lägre nivå. Säkerheten i TMP beror är olika för de olika protokollen.

Säkerhet i SNMP och SFMP

SNMP och SFMP använder ett enkelt säkerhetsschema baserat på en enkel autentiseringsprocess. Alla SNMPs datapaket och alla SFMPs order datapaket inkluderar ett communitynamnfält. Communitynamnfältet är en okrypterad oktettsträng som associeras mot en användargrupp. En agent kan bli konfigurerad så att olika användargrupper får olika nivå på dataaccessen.

Säkerhet i STMP

I STMP fås en låg nivå av säkerhet av att dataströmsstrukturen inte finns publicerad i någon standard. För att kunna tyda dataströmsstrukturen krävs information om hur de dynamiska

objekten är konfigurerade. Konfigurationsinformationen är endast kontaktbar via SNMP eller SFMP.

C2C

För C2C kommunikation används DATa Exchange (DATEX.ASN1) och Common Object Request Broker Architecture (CORBA). Dessa två protokoll anses nödvändiga av NTCIP för att bemöta variationen av krav för internsystemsdataöverföringar. Den senaste tiden har även eXtensible Markup Language (XML) börjat användas för C2C kommunikation. Att använda tre olika protokoll i ett nätverk är inget problem, det är bara låta några av centralerna agera bryggor eller översättare mellan de olika protokollen. Nedan följer beskrivningar av DATEX.ASN1, CORBA och XML.

I C2C nätverk tillåts varje system fråga efter alla tillgänglig information från något eller alla andra system. Varje system kan konfigureras att antingen svara eller neka en fråga. Data som skickas kan innehålla information eller ett kommando som utför en/flera handlingar. En användare kan även skapa prenumerationer på data, om de vill ha en viss sorts data med jämna mellanrum.

C2C kommunikation kräver peer till peer nätverksförbindelse mellan inblandade datorer. Normalt så är nätverket ett LAN, WAN eller en ring-upp (dial-up) anslutning. Alla sorters kommunikationslänkar kan användas så länge Internets transport och routing protokoll (TCP/IP och UDP/IP) kan användas.

Att ha i åtanke vid C2C kommunikation är att vare sig DATEX.ASN1, CORBA eller XML är en komplett lösning. För DATEX.ASN1 och CORBA är standarderna som definierar den data som ska överföras inte helt fastställda och för XML har inte branschen kommit överens om exakta regler för hur data ska överföras. Detta gör att det finns stor chans/risk att ett projekt måste genomföras i ett senare skede för att uppdatera mjukvaran och uppnå ett exakt användande av en standard.

DATEX.ASN1

DATEX.ASN1 är en ISO standard utvecklad av en av NTCIP: s arbetsgrupper. Det använder sig av fördefinierade meddelanden som överförs av Internet protokoll (TCP/IP och UDP/IP) i ett peer till peer nätverk och är designat för att tillhandahålla enkla och kostnadseffektiva lösningar för basbehov. Det är speciellt välanpassat för:

- System som kräver snabba realtidsöverföringar
- System med begränsad kommunikationsbandbredd men hög dataöverföringsvolym
- System med oregelbundna händelsedrivna överföringar över ring-upp (dial-up) länkar
- Icke-objekt orienterade system

Vid prenumerationer kan DATEX.ASN1 specificera om data ska skickas en gång, periodiskt eller direkt vid en inträffad händelse som är specificerad i prenumerationen. Varje prenumerationsmeddelande har ett korresponderande publikationsmeddelande. Om inte prenumerationen är en engångsföreteelse så kommer data automatiskt bli ”publicerat” fram

tills prenumerationen blir avbruten eller tills ett fördefinierat stoppdatum i prenumerationen inträffar.

I dagsläget används DATEX.ASN1 i ca hälften av systemen som använder sig av NTCIP: s standard.

CORBA

CORBA är ett protokoll för generell användning baserad på en standard med samma namn från dataindustrin. För objektorienterade system erbjuder det en högre nivå av integration och några tjänster som inte erbjudas av DATEX.ASN1, men det passar inte bra för nära realtidsapplikationer och dåligt ihopkopplade system.

Vid användning av CORBA kan ett system automatiskt och dynamiskt ”upptäcka” andra systems datatillgänglighet och delade kontrolloptioner. Dessa andra system använder CORBA för att publicera sin kompetens och sina tjänster, acceptera frågor från auktoriserade klienter och leverera sin kompetens och sina tjänster till dem som efterfrågat dem.

I dagsläget används CORBA i ca hälften av systemen som använder sig av NTCIP: s standard.

Säkerhet

CORBAs säkerhets tjänster har följande funktioner:

- Använder autentisering
- Säkra kommunikationer
- Access privilegium
- Access prioritet
- Access rapportering

När en användare accessar en centrals data, loggar användaren först in i centralens Security Service (SS). Baserat på autentiseringen hos SS får användaren en accessnivå eller en prioritet tilldelad som styr användarens tillgång till centralens apparater, händelser och tjänster. Användaren förblir inloggad tills den uttryckligen loggar ut genom SS: n. Användaren kan hela tiden kontrollera sin login status, inkluderat accessnivå och prioritet.

SS:en upprätthåller säkerhetsaccessen enskilt för varje användare. Varje användare tilldelas privilegium och prioritet av systemadministratören. Accesstilldelning är per apparat och metod/attribut privilegium är per apparattyp. Accesstilldelning för tjänster är per tjänst och metod/attribut privilegium är per tjänstetyp. Accesstilldelningar för händelser är endast per händelsemetod/attribut.

När säker kommunikation krävs mellan centraler använder sig SS av säkerhetsprotokollet Secure Socket Layer (SSL). SSL tillhandahåller server autentisering, hemlighållande och integritet för kommunikation över TCP/IP. Serverautentisering tillåter klient applikationen att verifiera identiteten hos servern den kommunicerar med.

XML

Enkelheten, utbreddheten av XML-verktyg och den stora marknaden av kunnig personal har skapat ett intresse av XML. Det är speciellt välanpassat för system som kräver begränsade och enkla dataöverföringar över kommunikationslänkar med tillräcklig bandbredd och processorer med tillräckligt med processeringstid över. I dagsläget används XML av ytterst få system som använder sig av NTCIP: s standard.

23.2.9 Informationsskiktet

I NTCIP definieras data beroende på vilket subsystem det tillhör. För respektive subsystem används olika datalexikon, i dessa definieras vilka data som ska användas i detalj. Datalexikon finns för bland annat variabla skyltar, väderstationer, datainsamling och kollektiv trafik. Exempel på lexikon är Traffic Management Data Dictionary (TMDD), Advanced Traveller Information System (ATIS), Transit Communications Interface Profiles (TCIP) och Incident Management (IM). Aktuella lexikon i NTCIP är baserade på amerikanska apparater och metoder.

23.2.10 Användning

NTCIP används i dagsläget i USA, oklart om samtliga tänkbara applikationer används.

23.2.11 Tillgänglighet

NTCIP är fritt att använda.

23.3 Open Communication Interface for Road Traffic Control Systems (OCIT)

Open Communication Interface for Road Traffic Control Systems (OCIT) är en tysk arbetsgemenskap för standardisering inom området vägtrafikteknik. OCIT: s arkitektur fokuserar på Intelligenta Transport System (ITS), i förstahand med inriktning mot trafiksignaler, men det är även inriktat mot andra områden som trafikdetektorer och variabla skyltar.

23.3.1 Omfattning

OCIT: s ledtankar är för standardisering är:

- Standardiserade och öppna gränssnitt är en förutsättning för fabrikatsblandade system och således mer konkurrens

- Trots standardisering måste utrymme för konkurrens finnas, som förutsättning för innovations- och prestationsförmåga för trafikteknik
- Standardiseringsansträngningen baseras på regler och systemarkitektur för vägtrafikteknik som finns i Tyskland, Österrike och Schweiz, men har som mål att få internationell utbredning.

Dessa ledtankar gör att målet för OCIT: s standardisering är att åstadkomma kommunikationsgränssnitt för fabrikatsblandade system. Gränssnitten är de mellan komponenter, apparater och system. Standardiserat blir protokoll, funktioner och data som betjänas i gränssnitten. Inre egenskaper som systemuppbyggnad, applikationer och databaser som inte hänger samman med gränssnitten omfattas ej av OCIT: s arbete. Detta främst för att främja konkurrens och innovationskraft.

Den tekniska basen för OCIT: s gränssnitt är Internetteknologi, därför möjliggörs trafikmanagementsystem och vidsträcka nätverk som omfattar centraler och fältstationer.

23.3.2 Medverkande i OCIT

OCIT består av tyska grupperingar med skilda intressen och uppgifter men med det gemensamma att de alla är verksamma inom området vägtrafikteknik. De är organiserade i form av ett ”runt bord” där att alla har lika mycket att säga till om. Det runda bordets viktigaste funktion är att likställa krav och önskemål från städer och planeringsbyråer jämtemot den ekonomiska press som finns från leverantörers och kunders sida. Verksamma i OCIT är Open Traffic Systems City Association e.V (OCA), Verband ders Ing. Büros für Verkehrstechnik (VIV), OCIT Developer Group (ODG) och Open Communcation for Traffic Engineering Components (OTEC).

OCA är en sammanslutning av tyska städer vars främsta intresse är att säkerställa de krav på funktionssäkring och harmonisering som finns på OCIT: s gränssnitt samt att påverka industrins utvecklingsarbete.

VIV är en sammanslutning av tyska ingenjörsbyråer som arbetar med trafikteknik. Deras uppgift i OCIT är att arbeta med de rekommendationer som OCA har angående framtagning av OCIT-system och komponenter.

ODG är arbetsgemenskap av tyska företag som arbetar med trafikstyrningssystem och dess komponenter. Deras uppgift i OCIT är att åskådliggöra tekniska lösningsvägar och omsätta resultaten i tekniska specifikationer för sina system och komponenter.

OTEC är ett konsortium av företag för standardisering av kommunikation mellan komponenter i vägtrafikteknik. Deras uppgift i OCIT är att åskådliggöra tekniska lösningsvägar och omsätta resultaten i tekniska specifikationer för sina komponenter.

23.3.3 Protokoll i OCIT

OCIT är uppdelat i olika gränssnittsområden, de två som berör protokoll är Instations och Outstations. Där Instations gränssnitt är mellan centrala komponenter och system och Outstations gränssnitt är mellan central och fältapparater.

Instations

För Instations pågår arbetet med att fastställa gränssnitten, fastställt idagsläget är att gränssnitten kan ses som dataflöden mellan komponenter och system. Kraven på protokollet skiljer sig åt beroende på om tjänsten är automatisk eller manuell, datamängd och -sort. Vad man kommit fram till hittills är följande:

- Dataöverföringen ska orientera sig efter OSI-modellen
- Användning av XML för databeskrivningen
- Dataöverföringen ska kunna använda alla sedvanliga medier och telekommunikationstjänster. I första hand Ethernet LAN och WAN.

Outstations

För Outstations finns en kommunikationsmodell med protokoll fastställd, den beskrivs nedan.

Systemelement

Ett OCIT-Outstations system består av en eller flera centraler och OCIT-Outstations. Centralernas roll i systemet är att styra och/eller övervaka fältapparaterna. Med OCIT-Outstations menas fältapparater som håller OCIT: s standard för fältapparater. Kommunikationsmedium mellan fältapparaterna och centralerna är ej standardiserat, utan fritt för leverantör/beställare att besluta.

Systemarkitektur

Då kommunikationsmediet mellan fältapparater och centraler ej är standardiserat kan ej några överföringstider garanteras. Därför måste alla tidskritiska styrningsuppgifter ske i fältapparaterna och inte genom kommunikation mellan central och fältapparat, detta kallas decentralt system. OCIT-Outstations har därför en processor som ska kunna behärska komplexa situationer på lokal nivå och kunna bearbeta vederbörliga data. I OCIT-Outstations definition förutsätts decentral arkitektur. Ett exempel på sådan arkitektur är ett trafiksignalsystem som kan registrera och bearbeta uppmäta trafikmängder samt hantera komplexa trafikberoenden.

Meddelanden och data blir bara överförda när bestämda händelser sker. Denna egenskap är en förutsättning för att kunna använda nätverkstekniken i OCIT.

Kommunikationsmodell

Dataöverföringen orienterar sig efter OSI-modellen. I skikt fem till sju används det egenutvecklade OCIT-Outstation protokollet Basis Transport Paket Protokoll Layer (BTPPL) som beskrivs nedan. I skikt fyra används standardprotokollen TCP och/eller UDP. Normalt stöder fältapparater både TCP och UDP, men vissa resursfattiga apparater stödjer enbart UDP. I skikt tre används standard IP och skikt ett och två är ej standardiserade.

OSI-skikt	OCIT: s protokoll
7	BTPPL
6	
5	
4	TCP UDP
3	IP
2	Fritt valbart, ex PPP
1	Fritt valbart

Tabell 14 Sammanställning av protokoll använda av OCIT

Skikt 1-2

Dataöverföringen baseras på telekommunikations standarder och alla sedvanliga medier och telekommunikationstjänster i skikt 1 och 2 kan användas. Vilket förbindningsprotokoll som används i skikt 2 styrs av vilket överföringsmedium och vilken överföringsinriktning som valts i skikt 1.

Skikt 3 (IP)

I skikt 3 används uteslutande standard IP, vilket gör det principiellt möjligt att ”routra” meddelanden från apparat till apparat eller till andra systemdelar.

Skikt 4 (TCP/UDP)

I skikt 4 kan TCP och UDP användas. Bägge protokollen används med respond respektive utan respond, mer om detta nedan.

För OCIT-Outstations är två portar för TCP och UDP nödvändigt. En port används för paket med låg prioritet (PLP) och en används för paket med hög prioritet (PHP). Bägge portarna används av både UDP och TCP. Vilken port som används är valbart och beror på hur viktigt paketet är. Svaret skickas till den port paketet kom från, med samma protokoll som användes när paketet mottogs. När ett paket skickas med UDP och svaret kräver mer än 4 kB, skickas ett felmeddelande som svar, då UDP inte klarar att hantera större paket än 4 kB. Normala meddelanden (< 4kB) kan överföras av TCP eller UDP, vilket som används väljs av centralen. I enkla apparater utan TCP-implementering används UDP.

UDP med respond

Vid en överföring med UDP skickas paketet från klient via en av portarna, mottagaren sparar jobbnummer, port och ip-adress. Användningen av jobbnummer säkerställer att det kan skickas flera ordrar från en port utan att det behövs vänta på svar från den första ordern.

Paketet mottas och bearbetas av tjänaren. För bearbetningen måste jobbnummer, sändarens IP-adress och port sparas tillfälligt för att ett svar ska kunna skickas. Om samma port och jobbnummer kombination uppträder ännu en gång under bearbetningen är det fritt valbart för implementeringen om den ignorerar ordern eller om den bearbetas igen. Så fort en order är bearbetad, skickas ett svar tillbaka med original jobbnummer till originalporten. Om det efter detta avskickande kommer en order med samma jobbnummer och port måste tjänaren bearbeta den på nytt.

Tjänaren skickar tillbaka svaret (respondpaketet) till adressen (jobbnummer + IP-adress + port) därifrån paketet kom. Om klienten inte mottagit ett svar när timeout tiden (25s) gått ut skickas paketet igen. Efter en andra timeout anmäls paketet (orden) som felgånget och det meddelas skickande program. Klienten vet då inte om orden ej genomförts, om orden genomförts men svaret förlorats eller om orden befinner sig i väntekö. Det är då klientens uppgift att besluta om orden ska upprepas eller ignoreras. Direkt när ett svar skickas tillbaka eller när den andra timeouten har skett överförs motsvarande meddelandet till programmet som skickat orden. Efterföljande svar, som är försenade, ignoreras helt.

För att skicka ett paket används ett ”request”-paket och för svaret används ett ”respond”-paket.

UDP utan respond

Ett paket skickas via någon av portarna, paketet mottas och bearbetas av tjänaren.

TCP med respond

Före att paket överförs över TCP, kontrolleras om en TCP-kanal finns öppnad. Är ingen kanal öppnad, öppnas en. Beroende på ordens viktighet skickas paketet genom den lågt respektive den högt prioriterade porten. Jobbnummer överförs när det behövs hos multithreadedtjänare och –klienter. Kanalen är minst öppnad till att ett svar kommer eller en timeout inträffar. Under orderutförandet måste det prövas om kanalen existerar som tidigare, om den inte gör det avbryts orden. Kanalen öppnas först igen för nästa order.

Svar skickas tillbaka den port från där sändningen utgick. Under bearbetningen är kanalen öppnad. Även i TCP skickas jobbnumret tillbaka i svaret. När tjänaren inte kan skicka tillbaka svarsmeddelandet, förkastas det och kanalen försöks inte öppnas på nytt.

I porten varifrån paketet skickades väntar klienten på svar. Kommer inget svar efter den första timeouten, skickas paketet igen. Efter en andra timeout anmäls paketet (orden) som felgånget och det meddelas skickande program. Klienten vet då inte om orden ej genomförts, om orden genomförts men svaret förlorats eller om orden befinner sig i väntekö. Det är då klientens uppgift att besluta om orden ska upprepas eller ignoreras. Direkt när ett svar mottas eller när den andra timeouten har skett överförs motsvarande meddelandet till programmet som skickat

orden. Det är inte nödvändigt att kanalen stängs efter svar skickas. Därför är det viktigt att klient och tjänare är programmerade så att de reagerar korrekt om kanalen stängs.

För att skicka ett paket används ett ”request”-paket och för svaret används ett ”respond”-paket.

TCP utan respond

TCP utan respond är möjligt.

Skikt 5-7 (BTPPL)

BTPPL omfattar:

- Ram uppbyggnad
    - Header
    - Serialisering av data
    - Provsummor (Fletchers algoritm, SHA-1)
- Avlöpning/Utveckling av metoduppmaningar
    - Funktioner med återställandeparameter
    - Funktioner utan återställandeparameter
- Metod för byte av OCIT-password

BTPPL omfattar ej:

- Metoder för betjäning av apparatfunktioner
- Definitioner av skikten under IP i OSI-modellen
- Metoder för att spara data.

BTPPL är ett symmetriskt protokoll. Det görs ingen principiell skillnad mellan fältapparat och central. Alla deltagande apparater är både tjänare och klient. Därför är det utanvidare möjligt att en fältapparat kan skicka ordar till en annan fältapparat.

BTPPL använder såkallade asynkrona metoduppmaningar. Där anslutna apparater blir uppmanade genom protokollet att utförda en viss funktion (metod). Anledningen till att asynkrona metoduppmaningar används är att de kräver avsevärt mycket mindre resurser än synkrona metoduppmaningar.

De definierade funktionaliteterna delas i ”Objekttypen”, ”ObjektIds” och ”Methoden”. Uppdelningen har följande bakgrund: I alla apparater finns det en lång rad med element som är mer eller mindre oberoende av varandra. I en trafiksignal finns det bland annat befallningar, mätställen och verksamhetsdagböcker. Varje element utgör en objekttyp. Oavsett om de existerar som fysikt objekt betraktas de logiskt som objekt. Alla dessa objekt kan anropas enskilt och har egna funktioner (metoder). Av vissa objekttyper finns det apparater med flera lika objekt, för att skilja dessa har varje objekt ett entydigt objektId. En funktion identifieras således av en kombination av Objekttyp, ObjektID och Methode.

Ramuppbyggnad i BTPPL

Jämfört med andra likvärdiga protokoll så har BTPPL en liten ram. Vilket leder till kortare överföringshastigheter och/eller ett lägre bandbreds behov.

Tids tillordning

- Aggregerade och mellanbuffrade data överförs med tidstämpel
- Aggregerade data överförs med den klocktid (tidstämpel) som är vid intervallets början
- Mellanbuffrade data överförs med klocktid (tidstämpel) vid framträdande av en händelse

Tidstämpeln är ingen beståndsdel som tillhör BTPPL utan det hör till det respektive objektet. Som format för tidstämpel används UNIX-Kodering. Koderingen sparar antalet sekunder sen 1/1 1970 i en 32 bitars variabel. Denna kodering stöds i princip av alla operativsystem, den är även kompakt och förenklar sorteringen av händelser. Att tänka på är att detta tidsformat löper över 19/1 2038. Detta problem är åtgärdat för kommunikationen i OCIT-Outstations genom att 32-bitars variablen enkelt nog bara räknar vidare. Detta gör att det blir problem först omkring år 2100.

Logisk tillordning

Svar på uppmaningar kan ske i annan tidsföljd än den de kommit i. Den logiska tillordningen mellan order och svar säkerställs genom BTPPL asynkrona Call - Respond mekanism.

Kodering av data

För Kodering av data används ett för OCIT-speciellt utvecklat format av XDR (RFC 1014), där ett antal förändringar genomförts för att spara bandbredd.

Övrigt

BTPPL har relativt låga krav på kommunikations hårdvaran, exempelvis kräver protokoll bara lite förvaringsutrymme. Detta gör att det även är aktuellt att använda för implementeringar i enkla apparater alternativt apparater med högt kostnadstryck.

Funktioner och objekt

Alla funktioner som är utförbara över OCIT-Outstations måste genomföras på samma sätt av likartade apparater, för att garantera enhetliga systemfunktioner. Det skiljs mellan OCIT-Outstations objekt och tillverkarobjekt.

- OCIT-Outstations objekt finns dokumenterade av OCIT och fastställer en standard. Alla likformiga OCIT-Outstations genomför funktioner bundna med dessa objekt på samma sätt.
- Tillverkarobjekt fastställs av leverantören för användning i egna system eller projektspecifikt. För att garantera ett ostört användande måste genomförandet följa ett regelverk. Här finns möjligheter för leverantörer att skapa saknade, ej förutsedda och

projektspecifika funktioner. Detta ger möjligheter till prestationsskillnader mellan leverantörer.

För OCIT-Outstations likformiga apparatfunktion finns nödvändiga objekt och egenskaper dokumenterade. Varje leverantör kan fritt välja vilka grundfunktioner deras apparater ska ha och dokumenterar detta.

Säkerhet

Överföringssäkerheten sköts i skikt 4 av TCP och UDP, beroende på vilket protokoll som används i skikt 2 kan överföringen även säkras där. Centralerna i OCIT-system är ofta anslutna till något nät, som exempelvis Internet eller intranät, där ett obekant antal användare har tillgänglighet. Detta gör att obehöriga kan komma över känslig information, därför kan även data säkras i BTPPL. Detta görs genom att dataöverföringen delas upp i icke säkerhetsrelevant kommunikation och säkerhetsrelevant kommunikation.

- **Icke säkerhetsrelevant kommunikation,** som övervägande delen av dataöverföringarna är, skyddas bara mot oavsiktliga överföringsfel och fel ledda UDP-paket. Denna säkring sker genom Fletchers algoritm, som är en enkel provsummealgoritm. En sådan säkring kräver endast 2 byte per paket.
- **Säkerhetsrelevant kommunikation** skyddas jämt mot avsiktliga intrång genom algoritmen SHA-1. SHA-1 är et så kallat provsummeförförande, där orättmätiga överföringar blir upptäckta och bortkastade. I andra sammanhang används SHA-1 för digitala underskrifter och det är allmänt erkänt för att vara säkert. För överföringssäkringen krävs egna passord (OCIT-password) som prövas i fältapparaterna. Användningen av detta förfarande har fördelen att ingång till system inte behöver ske genom en brandvägg.

Reaktionstid

Vid överföringar som kvitteras finns det en timeout tid, som tar hänsyn till maximal förväntad reaktionstid. I OCIT används samma timeout tid, 25 sekunder, för alla kvitterade överföringar.

Adresser

Fältapparater och centraler kommunicerar med varandra genom IP-adresser. I ett verksamhets nät måste således varje enskild fältapparat ha en entydig IP-adress. I första hand används egenförvaltade adresser. Äkta Internetadresser kostar pengar men priset är överkomligt, det är det höga behovet av adresser som gör det alternativet orealistiskt. Dessa ”fältapparat nät” är oftast stjärnformade och använder egna ledningar. Varje apparat har ett eget entydigt hostnamn, som förvaltas i en central genom en namnserver.

Databeskrivning

I OCIT-Outstations används Extensible Markup Language (XML) för databeskrivningen.

Topologiskstruktur

Vilken nätverks topologi som används i OCIT är fritt valbart. Vanligtvis används stjärntopologin.

23.3.4 Användning

I dagsläget används OCIT i två testområden i de tyska storstäderna Frankfurt och Dortmund, där testas kommunikation med hjälp av OCIT-Outstations gränssnitt. Annars är som tidigare nämnts OCIT: s arkitektur fokuserad på ITS och förbered för användning inom en mängd olika områden (exempelvis information, parkering, landsort). Typiska uppgifter är betjäning och övervakning av apparatfunktioner på distans, varvid ögonblickliga kvitteringar, reaktioner och felbehandlingar sker.

23.3.5 Tillgänglighet

För att få använda sig av OCIT krävs medlemskap i OCIT, kostnaden för medlemskap är ej känd.

23.4 Technische Lieferbedingungen für Streckenstationen (TLS)

Technische Lieferbedingungen für Streckenstationen (TLS) är en tysk standard med målet att enhetligt fastställa funktionella krav och gränssnitt för apparater som används för att samla in och behandla trafikinformation. Detta görs för att apparater från olika leverantörer ska ha till stor del samma prestationsförmåga och därmed enkelt ska gå att jämföra. För tillverkarna av apparater ska TLS tjäna som avgränsning av vilka egenskaper deras apparater ska ha och möjliggöra fri konkurrens.

23.4.1 Omfattning

I TLS definieras funktionella krav och gränssnitt för apparater som styr variabla skyltar och samlar in trafikdata respektive omgivningsdata. Information, inrapporterad från bland annat polis, vägbyggnations- och trafikmyndigheter till kartläggningssystem ska kunna tas tillvara och påverka styrningen av variabla skyltar. Utformningen av vägstationer med avseende på energiförsörjning, klimatförhållanden, överspänningsskydd, etcetera är definierat.

TLS är till stor del anpassat och framtaget för kommunikation och informationshantering kring det tyska motorvägsnätet. Mer om detta nedan, under Systembeskrivning.

23.4.2 Medverkande

TLS är framtaget av den statliga tyska förvaltningen Bundesanstalt für Straßenwesen (BASt) i samarbete med industrin och delstatsförvaltningen (Länderverwaltung).

23.4.3 Systembeskrivning

Nedan ges en kortfattad beskrivning av det system som TLS är anpassat för.

Systemnivåer

På grund av den rumsliga utbredningen av det tyska motorvägsnätet och andra omständigheter så är nätverket uppdelat i flera enskilda regionala nätverk. För att kunna behärska den förväntade datauppkomsten är varje regionalt nätverk uppdelat i flera hierarkiska nivåer, se tabell 15 för de olika nivåerna och dess roll.

Nivå	*Inrättning*	*Plats*
1	*Trafikräkningscentral*	*Central punkt i motorvägsnätet i en region*
2	*Undercentral, tjänar exempelvis till styrning av variabla skyltar*	*Exempelvis i motorvägsmästeriet eller i trafikräkningscentralen*
3	*Styrmodul och överföringssystem i den lokala stationen*	*Vägstation*
4	*Dataregistrerings- och datautgivningsapparater med I/O-koncentratorer för lokal data aggregering, för utvärdering av data, respektive för överlämnande av parametrar och ställkommandon*	*Vägstation*

Tabell 15 Hierarkiska nivåer i TLS (Källa: TLS utgåva 2002)

Trafikräkningscentralen kommunicerar med undercentralen över fjärrbussen, undercentralen kommunicerar med stationens styrmodul över öbussen och styrmodulen kommunicerar med de olika dataregistrerings- och datautgivningsapparaterna över lokalbussen.

Styrmodulen och dataregistrerings- och datautgivningsapparater i nivå 3 och 4 ryms i regel i ett och samma vägskåp.

Funktionsfördelning

Varje av de ovan nämnda nivåerna har speciella funktioner att uppfylla. Funktionerna ska avstämmas efter varandra och fördelas så att överföringsbehovet inte överstiger överföringskapaciteten. Endast data som behövs i nästa nivå ska vidarebefordras dit.

Nivå 1 och 2 funktioner beskrivs ej i denna rapport, då de har ringa relevans. De finns beskrivna i Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen.

Nivå 3 och 4 huvudfunktioner är följande:

Styrmodul:

- Styrning av datautbytet mellan undercentral och I/O-koncentrator
- Styrning av begäransrytm och överföringsproceduren för I/O-koncentratorerna på lokalbussen

I/O-koncentrator:

- Registrering och aggregering av trafik- och omvärldsdata från anslutna sensorer
- Vidarebefordra styrkommandon till variabla skyltar
- Funktionsövervakning och statusmeddelanden

Överföringsnät

För dataöverföringen mellan vägstation och undercentral finns i regel ett kabelpar (BAB-Streckenfernmeldekabels) till förfogande, där data kan skickas i halvduplex med hastigheten 1200 Bit/s. Dataöverföringen inom vägstationen sker med hjälp av en buss förbindning som består av två tvinnade ledningar som följer standarden RS485.

23.4.4 Kommunikationsmodell

TLS kommunikationsmodell orienterar sig efter OSI-modellen. I TLS används ett eget protokoll som motsvarar skikt 2, 3 och 7. Skikt 4-6 saknar motsvarande egenskaper i TLS. Skikt 2, 3 och 7 beskrivs var för sig nedan.

OSI-skikt	TLS
7	TLS skikt 7
6	Inget
5	
4	
3	TLS skikt 3
2	TLS skikt 2
1	Valbart

Tabell 16 Sammanställning av protokoll i TLS

23.4.5 Logik

TLS är ett master/slav protokoll. Mastern styr dataöverföringarna till och från de i hierarkin lägre slavarna. Vilken hierarkisk nivå som är master varierar beroende på förbindelse. Vid förbindelse mellan trafikräkningscentral och undercentral är trafikräkningscentralen master och undercentralen slav. Vid förbindelse mellan undercentral och styrmodul är undercentralen master och styrmodulen slav.

23.4.6 Skikt 2

I skikt 2 används enbart format klass FT 1.2 enligt standarden IEC 60 870-5-1 med de huvudsakliga egenskaperna:

- Hammingdistans 4
- Asynkron
- Byte orienterad
- Endast den osymmetriska överföringsproceduren tillåts
- All data kodas binärt

Meddelande

Det används tre olika typer av meddelande i TLS, långa meddelande, korta meddelande och kvitteringstecken. Långa meddelande har ett datafält med variabel längd. Korta meddelande har inget datafält och har en fast längd på 5 byte. Kvitteringstecken är en byte med värdet E5h.

De långa och de korta meddelandena begränsas av ett start- och ett sluttecken. I det långa meddelandet skickas start tecknet igen som byte nummer fyra. Som starttecken används 68h av det långa meddelandet och 10h av det korta. Bägge använder 16h som sluttecken.

I det långa meddelandet används en byte för att tala om meddelandets längd, denna byte finns med två gånger i meddelanden så totalt används två byte för att ange längden. Längd uppgiften är datafält inklusive styr- och adressbyte. Dessa två bytes skickas som byte två och tre i meddelandet.

Styrbyten innehåller funktioner som reglerar förbindningen mellan en primär och en sekundär station. Adressbyten innehåller, oavsett dataflödesriktning, alltid den sekundära stationens adress. När alla sekundära stationer skall nås har adressbyten värdet FFh. På den lokala bussen måste slavarnas adresser vara fritt inställbara, adresserna är mellan 1 och 199. Datafältet innehåller data som är relevant för de övre skikten. Datafältet består av ett variabelt antal databyte, maximalt får det vara 255 byte inklusive adressbyte, styrbyte och datafält.

Provsumma bildas av styr- och adressbyte för korta meddelande och av datafält, styr- och adressbyte för långa meddelande. Provsumman är den aritmetiska summan av dessa byts modulo 256.

Långmeddelande	Kortmeddelande	Kvitteringsmeddelande
Start 68h	Start 10h	E5h
Längdbyte	Styrbyte	
Längdbyte	Adressbyte	
Start 68h	Provsumma	
Styrbyte	Slut 16h	
Adressbyte		
Datafält		
Provsumma		
Slut 16h		

Tabell 17 Översikt av de olika meddelandetyperna och dess innehåll. (Källa: Technische Lieferbedingungen für Streckenstationen (TLS) utgåva 2002)

Överföringsregler

Regel 1: Vilotillstånd på ledningen motsvaras av 1-signal

Regel 2: Varje tecken har en startbit (0-signal), 8 informationsbitar, en jämn paritetsbit och en stopbit (1-signal)

Regel 3: Mellan de olika tecknen är inget vilotillstånd tillåtet.

Regel 4: Ordningsföljden på användardatatecknen beslutas genom modulo 256 provsumma.

Regel 5: Mottagaren kontroller:

Per tecken: - Startbit, stopbit och jämn paritetsbit.

Per meddelande:
- Startttecknen i början och slutet av meddelandeheadern
- Likheten mellan de två längdbyten
- Om antalet mottagna tecken är L+6
- Meddelandeprovsumman
- Slutttecknet

Är en av dessa kontrolleringar är negativ så ska meddelandet kastas bort, i annat fall är det fritt för användaren att använda. Motsvarande kontrollering görs för korta telegram och kvitteringstecken.

Överföringshantering

Datatrafiken avvecklas genom så kallade primitives. En primitive bildar en obrytbar kombination av datasatser mellan primär- och sekundärstation. För dataöverföring används tre primitives, skicka/inget svar, skicka/konfirmera och begäran/svar.

Det finns två överföringsklasser. Överföringsklass 2 används för den normala begär cyklern och överföringsklass 1 är reserverad för händelsedata.

Avbrott i händelseförloppet

Det kan uppstå flera olika saker som orsakar ett avbrott händelseförloppet:

- RNR, en slav eller en master inte kan ta emot mer datapå grund av en intern flaskhals (exempelvis begränsad buffer). Mastern kräver inte i detta tillstånd att få användardata från slavarna. Meddelanden med funktioner som gör att slaven svarar med ett kvitterings- eller ett svarsmeddelande kan fortfarande användas då dessa meddelanden alltid tas emot av mastern. Slaven visar RNR genom att i ett av sina kvitterings- eller svarsmeddelande sätta en speciell bit till 1.
- Timeout, efter en viss tid efter att mastern skickat iväg ett meddelande och det inte fått svar eller kvittering skickas samma meddelande igen.

23.4.7 Skikt 3

Förmedlingsprincip

Till varje transit- eller slutstation löper meddelanden in och ut. Varje ingång och utgång hos en transit- eller slutstation tilldelas en port. Portarna beskriver därmed destinationsadress (ingångport) och från vilken utgångsport i den tidigare stationen meddelandet kommit från. Därmed hör varje överföringsavsnitt till en utgångsport och en ingångport.

De parvisa portarna används som adresselement i överföringsprocessen och betecknas som adress I och adress II. Ordningsföljden av dessa adresser anger vilken väg ett meddelande ska ta för att nå sin destination. Förmedlingsprocessen i stationerna använder sig inte av meddelandet, utan den aktuella destinationsadressen anges genom en pekare. Pekaren är en del av skikt 3: s meddelande del.

Ett överföringsavsnitt beskrivs av 2 byte, adresserna uppträder parvis. Adresspekaren pekar jämt på den aktuella destinationsadressen (Adress II) i överföringsavsnittet. Pekaren startar på värdet 0 i startstationens förmedlingsingång, efter varje nådd destination inkrementeras pekarvärdet, så att pekaren pekar på rätt överföringsavsnitt. När värdet i pekaren nått värdet i längdangivelsen har meddelandet nått slutdestinationen. För tillbakasändning speglas adressfältet.

Skikt 3: s meddelandeandel

Skikt 3: s meddelandeandel består av adressidentifiering och adressfält.

Adressidentifieringen består av tre delar: prioritetsbitar, pekare och längdangivelse. Det finns två olika prioritetsnivåer, prioritetsklass 1 och prioritetsklass 2. Dessa två klasser motsvarar överföringsskikt 1 och 2 i skikt 2.

Adressfältet består av maximalt sju adresspar, där varje adresspar beskriver ett överföringsavsnitt. Att sju är maximalt adresspar gör att en överföring kan ske över maximalt åtta nätverksstationer.

Om längd angivelsen är 0 sätts även pekaren till 0 och adressfältet faller bort. Därmed blir skikt 3: s meddelandeandel reducerad till endast 1 byte. Överföringen sker i detta fall över ett överföringsavsnitt och fungerar bara uppåt i hierarkin. Vid överföring på den lokala bussen är skikt 3: s meddelandeandel 1 byte, adresseringen hanteras då i skikt 2.

Adressfördelning

Masteradresser: 200-209
Adresser på mastersidan, som skapar en förbindelse master (undercentral, trafikräkningscentral) och slav (station, undercentral), är masteradresser. Om en undercentral eller trafikräkningscentral är master i flera delnätverk måste den ha flera masteradresser.

Slavadresser: 1-199
Adresser på slavsidan av stationer och undercentraler.

Adresser för extern användning: 210-254
Adresser som beskriver en applikation (interna användningar eller utgångsportar för PC-kort) eller förbindningar till enheter utanför det hierarkiska nätverket.

Adress till alla stationer: 255
Används för att adressera till alla enheter längs ledningsbussen. Att tänka på är att de enheter man vill nå är slutenheter, då en vidareförmedling inte är möjlig.

23.4.8 Skikt 7

Adressering

Fysiska adresseringsobjekt

En vägstation består av en styrmodul med ett modem, en eller flera I/O-koncentratorer och deras underordnande I/O-kanaler.

Logiska adresseringsnivåer

Datainnehållet från en vägstations I/O-kanaler som funktionellt hör ihop överförs tillsammans genom användande av logiska adresseringsnivåer. Vägstationers I/O-kanaler adresseras logiskt inom vägstationen med de två adresselementen funktionsgrupp (funktionsgruppe, FG) och data-slutapparat-kanal (Data-Endgeräte-Kanal, DE).

Funktionsgrupper infattar grupper av I/O-kanaler, datakällor eller –sänkor som utgör samma funktion. En funktionsgrupp kan ha sina I/O-kanaler fördelade i flera olika I/O-koncentratorer och I/O-kanaler tillhörande olika funktionsgrupper kan vara integrerade i en I/O-koncentrator.

DE är den logiska adressen till den minsta adresserbara enheten, I/O-kanalerna. Varje I/O-kanal tillhör entydigt en funktionsgrupp och tilldelas ett valbart entydigt DE-nummer.

Adressering av systeminterna nyheter

För överlämnande av parametrar och förfrågningar om fel- och statusinformation, det vill säga för överlämnande av systemdata till hårdvaruenheterna, måste I/O-koncentratorerna respektive styrmodulen adresseras. Eftersom den logiska adressen funktionsgrupp inte är identisk med hårdvaruenheterna I/O-koncentrator respektive styrmodul finns en funktionsgrupp som heter System (FG, 254), vars I/O-kanaler är I/O-koncentratorer och styrmodulen. Den logiska adressen (DE) för dessa I/O-kanaler är inte fritt valbara utan motsvaras av skikt 2 adressen på lokalbussen. Systemstyrningen i styrmodulen adresseras med FG 254 / DE 0. Övriga adresseras med FG 254 / DE n, där n är dess skikt 2 adress på lokalbussen.

Samlings- och gruppadressering

När ett antal DE: s ska överföra samma datablock sker detta i funktionsgruppen systemstyrning med hjälp av samlingsadressering respektive i användarfunktionsgrupperna med hjälp av samlings- och gruppadressering. Bildande av DE-grupper förutsätts därmed logiskt, detta sker genom tilldelning av DE-nummer under projekteringen av vägstationen och är inte bundet till en rumslig tillordning.

För en funktionsgrupp är sju grupper med 30 DE: s möjligt. Upp till detta antal kan ett godtyckligt antal DE: s anropas som en grupp. Det är även möjligt att adressera samtliga DE: s i alla grupper, som hör till samma funktionsgrupp, gemensamt.

En klusterkanal är en extra I/O-kanal hos en I/O-koncentrator som används vid behov. Med en klusterkanal blir ett kluster av I/O-kanalers bestämda funktioner tilltalade. I/O-kanaler som bildar ett kluster hör funktionellt ihop. Användning av klusterkanaler är fördelsfull när en funktionsgrupps I/O-kanaler har en funktion som styrs gemensamt. En klusterkanal är en självständigkanal, som tilldelas ett DE-nummer. Det finns maximalt en klusterkanal per funktionsgrupp och I/O-koncentrator. En klusterkanal överför enbart användningsdata.

Klusterkanaler genererar inga negativa kvitteringar när de får data avsett för I/O-kanaler via en samlingsadress. DE-kanaler genererar inga negativa kvitteringar när de får data avsett för klusterkanalen. Därmed blir en adressering med samlingsadress möjlig utan att klusterkanalen måste uteslutas.

Adressering av grupper på lokal- och öbussen är bara möjlig i begäransriktningen, i svarsriktningen blir identiska data alltid överförda i block från varje DE.

Meddelandestruktur

När flera meddelanden ska skickas till samma mottagare vid samma tidpunkt kan dessa meddelanden packas samman och skickas i ett skikt 7 block. Ett skikt 7 meddelande består av en allmän header, en eller flera singelmeddelande headers (beroende på om flera meddelanden packas tillsammans) och DE-Block. Packning av meddelanden används endast på nivåer ovanför styrmodulen i vägstationen, således ej på lokalbussen.

Allmän header

Den allmänna headern används på öbussen, på den lokala bussen existerar den ej. Den innehåller enhetsnummer och antal singelmeddelande.

Byte 1 till 3, enhetsnummer, innehåller ett nummer som utmärker käll- respektive destinationsenhet. I hierarkin neråtgående (exempelvis trafikräkningscentral till undercentral meddelanden) meddelanden har destinationsenhet i enhetsnumret. I hierarkin uppåtgående meddelanden har källenhet i enhetsnumret. Varje enhet måste ha ett på nätverket entydigt enhetsnummer.

Enhetsnummer 0 accepteras av alla enheter oavsett tilldelat enhetsnummer. Det används för meddelanden med globaladress (exempelvis tidsynkronisering) och under projekteringsfasen då enheter inte fått något enhetsnummer.

Byte 4, antalet singelmeddelande, anger med ett tal hur många singelmeddelanden meddelandet innehåller, minimum är ett.

Singelmeddelande header

Singelmeddelande headern är kärnan i meddelandena och är alltid en del av dem. Singelmeddelande headern innehåller information över längden och tillordningen i aktuellt meddelande.

Byte 5, singelmeddelandes längd, anger antalet meddelandebyte i följande singelmeddelanden. Den räknar ej med sig själv.

Byte 6, funktionsgruppen, betecknar grupper av DE: s, som utgör samma typ av datakälla respektive –sänka.

Byte 7 är riktnings-/användningsidentifierare (ID). Bit 0 till 6, ID, kodar meddelandets uppgift. Speciella instruktioner för behandling av data ges, respektive en grov indelning av data beroende på sort. Bit 7 anger meddelandes riktning, 0: meddelandet skickas i begäransriktning, 1: meddelandet skickas i svarsriktning.

Byte 8, jobbnummer, tjänar till begäran-svars-tillordning över alla nätnivåer. Varje meddelandekälla ger med hjälp av en egen algoritm sina meddelande ett jobbnummer. I svarsmeddelandena respektive kvitteringarna inkluderas samma jobbnummer.

Byte 9, antal DE-Block, anger antalet block i meddelandet som innehåller en enskilds DE: s data. Maximal antal begränsas av maximal meddelande längd och är 76.

DE-Block

Byte 10, längd på DE-blocket, anger antalet byte i det efterföljande DE-blocket. Längdbyten räknas ej med själv.

Byte 11, data-slutapparat-kanal (DE), är den logiska adressen för de minsta informationsmottagande eller utskickande enheterna. DE anger vilken eller vilka kanaler de följande byten hör till. Upp till 210 enskilda DE: s kan adresseras, resterande adresser används för gruppadressering respektive är fria.

Byte 12, typbyte, kännetecknar typen på efterföljande data respektive mer detaljerad betydelse av meddelandet. Typbyten kan definieras olika per funktionsgrupp och inom den per ID, dock eftersträvas om möjligt en överensstämmande definition.

Dataöverföring under drift

Krav på dataöverföringen

För att göra dataöverföringen entydig, säker och ställa överförd data tillförfogande snabbt finns en rad krav ställda. De redovisas nedan med TLS lösningar på kraven.

- **Ringa påfrestningar på överföringskanalen**, data överförs endast då det innehåller relevant information. En användare begär data endast när data inte skickas impulsivt eller när det inte är cyklisk data.
- **Säker överföring**, överföringen säkras, så långt som möjligt, genom kvitteringar respektive svarsmeddelanden.
- **Minimal överföringstid**, när möjlighet finns överförs information till flera DE: s i ett meddelande samt att flera meddelanden som ska till samma DE packas samman till ett meddelande.
- **Minimal reaktionstid på överföringsönskemål**, utgåendemeddelanden från vägstationerna blir överförda till centralen före andra meddelanden så att centralen undviker att begära utgående data.
- **Entydig tidstillordning**, Cykliskt aggregerade data överförs med tidpunkt från intervallstarten. Därmed låter sig sådana data entydigt tillordnas.
- **Prioritets tillordning**, meddelanden för en prioritet tilldelad, som överföringsstyrningen i skikt 2 utnyttjar.

Händelseklasser

För att ge bättre förståelse för datautbytet delas dataöverföringshändelserna i fyra klasser.

- **Spontan, enkelriktad överföring (Händelseklass 1)**
  Den spontana enkelriktade överföringen sker i begär- och svarsriktning. De kännetecknas av ett enskilt meddelande (från platsen där informationen framträdde)

ställs till förfogande hos mastern direkt vid framträdandet. Ingen kvittering sker i skikt 7.

- **Begärda överföringar (Händelseklass 2)**
  Begärda överföringar indikeras av de högre hierarkinivåerna och dess roll är att överföra data från de lägre nivåerna till de högre. De kännetecknas av ett kort begäransmeddelande och ett svarsmeddelande med efterfrågad data.
- **Kommando överföring med svarsmeddelande (Händelseklass 3)**
  Kommando överföringar indikeras av de högre hierarkinivåerna och tjänar dataöverföringen i de nedre nivåerna. De kännetecknas av ett meddelande som innehåller användardata för en informationssänka i de lägre nivåerna och ett svarsmeddelande innehållande de nya drifts- och kopplingstillstånd.
- **Parameteröverföring med positiv kvittering (Händelseklass 4)**
  Parameteröverföringar med positiv kvittering indikeras av de högre hierarkinivåerna och tjänar dataöverföringen i de nedre nivåerna. De kännetecknas av ett meddelande som innehåller användardata för en informationssänka i de lägre nivåerna och ett kvitteringsmeddelande som kvitterar att data mottagits.

Information till vägstationerna kan skickas med flera av de ovan nämnda händelseklasserna.

Regler för dataöverföring

DE-block strukturer som beskriver tids sammanhängande händelser i en I/O-koncentrator överförs i ett singelmeddelande om funktionsgrupp och ID är identiska.

Överföring av cykliska data

Cykliskt uppkomna data skickas vid slutet av mätintervallet till centralen utan en begäran från användaren (händelseklass 1). Centralen kan ställa intervallängden efter aktuella behov genom inställningskommandon. Det är även möjligt för centralen att skicka en begäran om cykliskt uppkomna data, det blir då resultaten från det senast avslutande mätintervaller som skickas.

Vid omfångsrika data och långa mätintervall är överföring vid begäran (händelseklass 2) att föredra för att minska den oregelbundna belastningen på överföringskanalen. Vid cykliska data blir det använda mätintervallet synkroniserat. Som referenspunkt används dygnsväxlingen (00.00), på grund av det måste intervallängden vara en hel del av 24h.

Överföring av mätvärden

För överföring av mätvärden finns det två alternativ. Det enklaste alternativet är det med cykliskt överförda mätvärden, vilket utförs på samma sätt som överföring av cykliska data (beskrivs ovan). Det andra alternativet är överföring efter begäran.

Överföring av inställningskommandon

Inställningskommandon tjänar till ändringar av variabla skyltar, driftsparametrar hos vägstationer respektive DEs eller för utlämnande av övriga kommandon för driftsstyrningsinstitutioner. Överföringen sker efter händelseklass 3.

Överföring av parametrar, resultat och liknande

Principiellt överförs all information efter att ändring respektive intervallslut till centralen, så att begäran av data endast är nödvändig vid specialfall. Begärningar av önskade data sker efter krav från centralen med ett begärmeddelande, vägstationen respektive I/O-koncentratorn svarar med önskade data (händelseklass 2).

Överföring av tidstämpel

DE-blocket ”tidstämpel” tjänar till den tidsliga tillordningen av meddelanden i svarsriktning. Det skickas tillsammans med andra DE-block innehållande händelsedata och anger tidpunkten för händelsen som föranlett meddelandet. Detta gör det möjligt för centralen att dokumentera tidpunkten för händelsens inträffande.

Användning av samlingsadresser för DEs

Byten DE i meddelandena kan användas för adressering av enskilda kanaler eller för samlingsadressering. Samlingsadressering är möjlig endast i begäransriktning.

Prioritetsanvisningar

Överföringsproceduren i skikt 2 möjliggör överföring med hög och låg prioritet. Svarsmeddelanden på begärningar erhåller samma prioritet som begäransmeddelandet. För andra meddelanden i svarsriktning gäller att fel- och frånfallsmeddelanden överförs med hög prioritet och normala resultatmeddelanden med låg prioritet. Avvikande är att meddelande tillhörande funktionsgrupp 4, som alla innehåller tidsstämpel med följenummer, alltid har den lägre prioriteten.

Routinginformation för skikt 3

En vägstation skickar alltid tillbaka sina svar på begärningar och kommandon genom speglad routing. För de spontat uppkomna meddelandena används projekterbara routingfält som finns i vägstationen. Standardmässigt projekteras ett routingfält för varje funktionsgrupp. Valbart är att projektera avvikande routingfält för enstaka funktionsgrupper. Dessa routingfält är ändringsbara per telegram.

Funktionsgrupper som inte har ett routingfält projekterat använder standard routingfältet. Är inte detta routingfält definierat skickar vägstationen meddelandet utan routinginformation till närmsta enhet tillhörande en högre hierarkinivå.

Dataöverföringar på lokalbussen (mellan styrmodul och I/O-koncentratorer)

Som primär informationskälla styr I/O-koncentratorerna till stor del dataöverföringarna på lokalbussen vad gäller tid och omfång. Styrmodulens uppgift är att förmedla datatrafiken mellan undercentral och I/O-koncentratorer och att iaktta systemmanagementet.

Varje I/O-koncentrator skickar vid utlöpandet av ett tidsintervall sina data med ändrade mätvärden, andra interna eller externa händelser till styrmodulen. Styrmodulen skickar vidare data direkt till undercentralen, eventuellt packas data först hos styrmodulen. Sammanslagning

av singelmeddelanden från olika I/O-koncentratorer med lika singelmeddelanden till ett singelmeddelande med alla DE-block kan ske men är inget krav.

Kommandon till inputkanaler, parameteranvisningar etcetera leder styrmodulen vidare till vederbörlig I/O-koncentrator.

Dataöverföringar på öbussen (mellan vägstation och undercentral)

Omfång och tidpunkt för dataöverföringar mellan vägstation och undercentral styrs av datakällorna på lokalbussen. Dataöverföringarna äger rum i passande händelseklass.

Störningsindikation/felanmälan

Meddelande om systemstörningar

Störningar i vägstationer som påverkar driften måste meddelas till centralen, detta görs genom felmeddelanden. Felmeddelandena kvitteras aldrig i skikt 7.

Meddelandet av störningar har tre uppgifter:

- Informera om den begränsade systemkapaciteten, så att exempelvis ersättningsstyrning av variabla skyltar kan tas i bruk.
- Informera nätanvändarnas servicepersonal, så att de kan göra återgärder för att undanröja störningen.
- Informera apparatleverantören över störningens natur och omfattning, över defekta delkomponenter, och så vidare.

Resultatöverföringar vid defekta kanaler

DE: s som är fallit ifrån skickar ingen mer data till centralen. Vid framträdandet av störningen meddelas centralen om den defekta kanalen, därmed förväntar den sig inga data. Spontant skapade meddelanden innehåller enbart information från de DE: s som kan leverera giltig data eller faller ifrån helt om inga DE: s kan leverera giltig data. Vid begäransmeddelanden skickas alltid ett svarsmeddelande. Svarsmeddelandet innehåller information från de DE: s som kan leverera giltig data, om ingen DE kan leverera giltig data skickas ett svarsmeddelande med antalet DE-block = ”noll”.

Störningar på öbussen (mellan undercentral och styrmodulen i vägstationen)

Kommunikationsstatusen blir känd för styrmodulen (vägstationen) med ledning av skikt 2. När styrmodulen inte blivit kontaktad (pollad) av undercentralen under en inställbar tid (1-10 min), växlar den kommunikationsstatusen till ”störd”. Vid återstart i skikt 2 protokollet och mottagande av RES 0, växlas statusen tillbaka till ”levande”. Tiden tills styrmodulen växlar till statusen ”störd” måste vara mindre än motsvarande tid hos undercentralen.

Störningar på lokalbussen (mellan styrmodul och I/O-koncentrator)

När I/O-koncentrator inte blivit kontaktad (pollad) av styrmodulen på 30 sekunder växlar den sin kommunikationsstatus till ”störd”. Tiden tills I/O-koncentratorn växlar till statusen ”störd” måste vara mindre än motsvarande tid hos styrmodulen. I kommunikationsstatus ”störd” eller ”obestämd” svarar I/O-koncentratorerna på begärningsmeddelanden men endast spontana meddelanden tillhörande funktionsgrupp 254 får skickas.

Upptäcker styrmodulen med hjälp av skikt 2 att en I/O-koncentrator fallit bort måste detta meddelas de högre hierarkierna inom 20 sekunder.

Negativa kvitteringar

Med negativa kvitteringar svaras begärningar som inte kunnats bearbetas i ordningsmässigt. Genom jobbnumret kan avsändaren se vilket meddelande som berörs.

23.4.9 Funktionsgrupper

De i TLS beskrivna funktionsegenskaperna är krav vid en implementering och måste finnas tillgängliga. Funktionsegenskaperna är uppdelade i olika funktionsgrupper.

En vägstation stödjer beroende på dess uppgift olika funktionsgrupper, dock är funktionsgrupp 254 alltid installerad. Totalt finns det 256 olika funktionsgrupper, i tabell 18 nedan, ses de olika funktionsgrupperna och dess ändamål.

Funktionsgrupp	*Ändamål*
0	*Reserverad för teständamål*
1	*Trafikdataregistrering*
2	*Axellastdataregistrering*
3	*Omgivningsdataregistrering (väder)*
4	*Styrning av variabla skyltar*
5	*Reserverad*
6	*Driftsrapporter och –styrningar av VLT-nätet*
7	*Anläggningsstyrning*
8	*Hastighetsövervakning*
9	*Tillflödesreglering*
10-15	*Reserverade för senare allmänförknippade definitioner*
16	*Väg-fordon-kommunikation*
17-127	*Reserverade för senare allmänförknippade definitioner*
128-253	*Fria för tillverkardefinierade funktionsgrupper*
254	*Systemstyrning (intern funktion)*
255	*Reserverade för speciella ändamål*

Tabell 18 Funktionsgrupper och dess ändamål (Källa Technische Lieferbedingungen für Streckenstationen (TLS) utgåva 2002

23.4.10 Tillgänglighet

TLS tillgänglighet är oklar, sannolikt är det en förhandlingsfråga med den tyska förvaltningen.