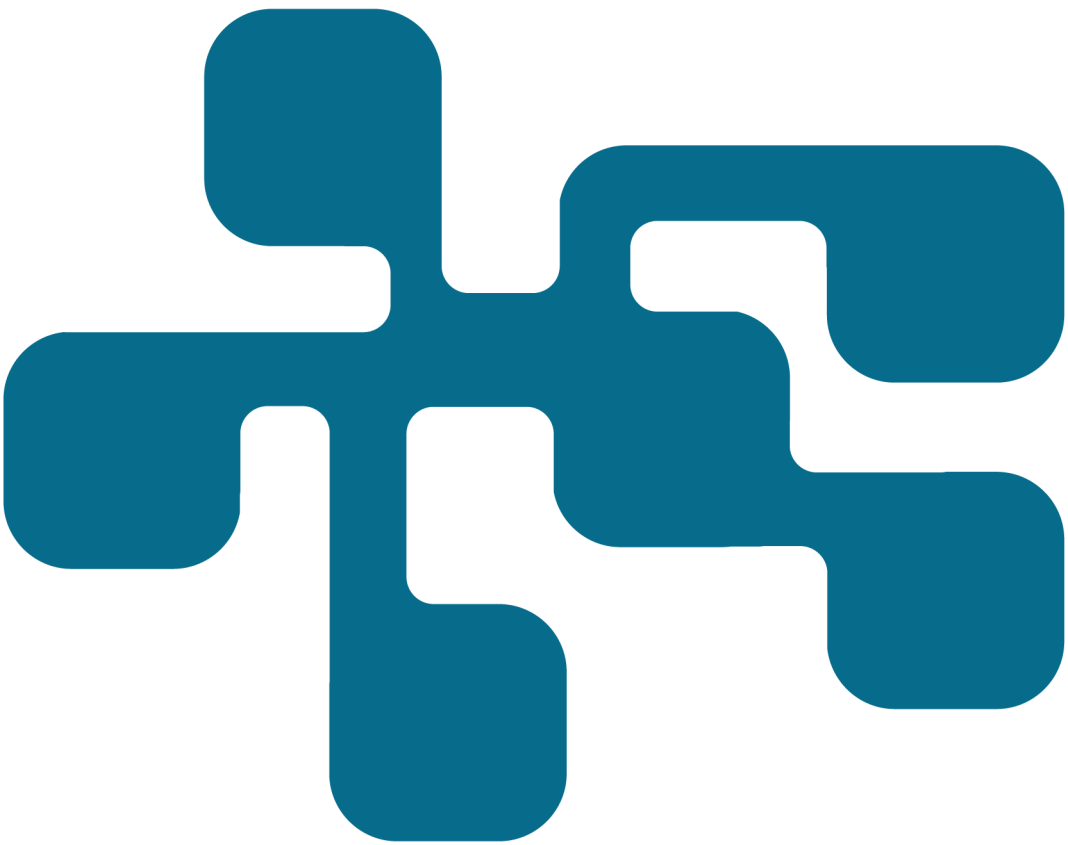
NCS3 - Industriella protokoll i Sverige

En översikt över protokoll inom industriella informations- och styrsystem i kritisk infrastruktur

Daniel Eidenskog, Björn Lindahl

FOI
MSB



FOI-R--4438--SE
MSB 2017-3717
ISSN 1650-1942

Juni 2017

Daniel Eidenskog, Björn Lindahl

NCS3 – Industriella protokoll i Sverige

En översikt över protokoll inom industriella informations- och styrsystem i kritisk infrastruktur

Titel	NCS3 – Industriella protokoll i Sverige
Title	NCS3 – Industrial Protocols in Sweden
Rapportnr/Report no	FOI-R--4438--SE
Månad/Month	Juni
Utgivningsår/Year	2017
Antal sidor/Pages	59
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E72104
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Industriella informations- och styrsystem använder en uppsjö olika protokoll beroende på faktorer som systemets ålder, leverantör, befintliga system och beställarens preferenser. Många sektorer inom kritisk infrastruktur använder industriella information- och styrsystem för att kontrollera kritiska processer, exempelvis inom dricksvattenförsörjning, avloppsrening, elproduktion och eldistribution.

Den här rapporten presenterar en studie över vanligt förekommande protokoll inom kritisk infrastruktur i Sverige. Studien består av två huvuddelar, först en intervjuserie följt av en litteraturgenomgång. Intervjuerna fokuserade på att samla in information om vilka protokoll som används, medan litteraturgenomgången gav information om respektive protokoll och deras egenskaper.

Resultaten visar att många olika protokoll används inom kritisk infrastruktur. Många organisationer använder en mängd olika protokoll, ofta beroende på historiska skäl såsom befintliga system och att olika delar av organisationen tidigare varit oberoende från varandra. Protokollvalet är sällan i fokus vid uppgraderingar och nyinstallationer, istället är det snarare systemets övergripande funktion och leverantörernas preferenser som styr valet av protokoll.

Nyckelord: ICS, industriella informations- och styrsystem, protokoll, kritisk infrastruktur.

Summary

Industrial control systems use a variety of different protocols depending on factors such as system age, supplier, dependencies, and buyer preferences. Many sectors within critical infrastructure, such as water supply and wastewater treatment as well as production and distribution of electricity, use industrial control systems to control critical processes.

This report presents a study of commonly used protocols in industrial control systems in Swedish critical infrastructure. The study consists of two main parts; a series of interviews followed by a literature review. The interviews aimed to gather information on what protocols are in use, while the literature review gave an overview of the protocols and their properties.

The results show that many different protocols are in use within critical infrastructure. Many organisations use a variety of protocols, often due to historical reasons such as legacy systems or previously independent branches of the organisation. The protocols are seldom in focus during upgrades or new installations. The selection of protocols is often the result of overall function combined with the suppliers' preferences.

Keywords: ICS, industrial control systems, protocols, critical infrastructure

Innehållsförteckning

1 Inledning

Industriella informations- och styrsystem använder en uppsjö olika protokoll, där valet av protokoll beror på olika faktorer såsom systemets ålder, leverantör, komponentval, befintliga system, beställarens preferenser och många andra aspekter. Industriella informations- och styrsystem används inom många sektorer, inklusive flera sektorer som utgör samhällskritisk infrastruktur, exempelvis vatten och avlopp, elproduktion och eldistribution.

Historiskt sett har tillverkare av styrutrustning ofta utvecklat egna protokoll för att möta de behov som respektive tillverkare har sett som viktigast inom respektive användningsområde. Även om tillverkarna i detta läge sätter sin egen prägel på protokollen så bestäms de övergripande egenskaperna i stor grad av det huvudsakliga användningsområdet, vilket har lett till att det finns ett antal protokoll som har liknande egenskaper inom respektive användningsområde.

Denna rapport beskriver en studie vars övergripande mål är att kartlägga och beskriva de vanligaste protokollen för industriella informations- och styrsystem som används inom kritisk infrastruktur i Sverige.

1.1 Syfte och mål

Syftet med studien är att ge en överblick över vilka protokoll som är vanligt förekommande i industriella informations- och styrsystem inom kritisk infrastruktur i Sverige. I denna överblick ingår även att ge en övergripande beskrivning av de protokollen som används enligt studien.

Studien är uppdelad i två delar, bestående av en serie intervjuer samt en litteraturgenomgång. Intervjudelen avses svara på följande forskningsfrågor:

1. Vilka protokoll förekommer och vilka är vanligast i styrsystem inom kritisk infrastruktur?
2. I vilka delar av systemen används protokollen och för vilka syften?

Litteraturgenomgången har genomförts för att samla in och sammanställa information om de protokoll som identifierats i intervjuerna.

1.2 Avgränsningar

Studien avser inte ge en komplett bild baserad på alla industriella informations- och styrsystem inom kritisk infrastruktur, då detta vore ett allt för omfattande arbete. Avsikten är i stället att nå en övergripande bild av protokoll inom kritisk infrastruktur genom att studera ett snitt genom ett antal olika verksamheter.

1.3 Läsanvisningar

Kapitel 2 tar upp de beskrivningsmodeller som används för kategorisering av protokollanvändning samt i protokollbeskrivningarna. Kapitel 3 beskriver metoden för studien. Kapitel 4 tar upp resultaten från intervjuerna medan kapitel 5 beskriver de identifierade protokollen. Kapitel 6 avslutar rapporten med en lista över ord och förkortningar.

2 Protokollstrukturer

Nätverk bygger ofta på en stor mängd protokoll för att sköta olika uppgifter i kommunikationen. Allt från hur den fysiska uppkopplingen sker – exempelvis elektriskt, optiskt eller med radio – till hur olika applikationer utbyter data med varandra.

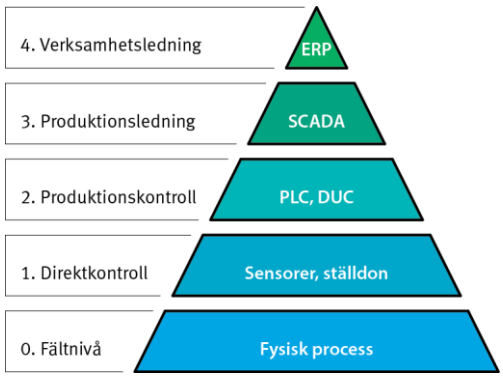
Det finns i regel ett flertal protokoll som löser principiellt samma problem på samma nivå, exempelvis IPX/SPX-sviten som användes i stor utsträckning i företagsnätverk innan TCP/IP-sviten fick den dominerande ställning den har idag. På samma sätt finns det ett stort antal protokoll inom industriella informations- och styrsystem som alla löser det fundamentala problemet att överföra status och styrsignalering mellan olika styrutrustningar.

Protokoll går att kategorisera på många sätt och utifrån många olika typer av egenskaper. I det här arbetet fokuserar kategoriseringen på användningsområde och lagerstruktur. Användningsområdena beskriver i vilka delar av ett industriellt informations- och styrsystem som protokollen används, medan lagerstrukturen avser protokollens relation till applikationen och andra protokoll som används i kommunikationen.

2.1 Referensmodell för styrsystem

I detta avsnitt presenteras en övergripande modell som syftar till att kunna beskriva de olika delarna i ett industriellt informations- och styrsystem. Utgångspunkten för modellen är hämtad från standarden *Enterprise-control system integration* (IEC 2013). Ursprunget till modellen kommer ifrån *Reference Model for Computer Integrated Manufacturing* (Williams 1989) och är även en standard under International Society of Automation (ISA 2010). Modellen kallas allmänt för Purdue-modellen då den ursprungliga referensmodellen skapades på Purdue-universitetet. Valet av modell baserades på att det är en accepterad modell för att beskriva industriproduktion ur ett helikopterperspektiv. Av den anledningen är modellen även användbar för verksamheter där distribution är i fokus.

Modellen delar upp en organisation i fem nivåer enligt figur 1. Vid varje nivå finns en beskrivning av vilken verksamhet som respektive nivå ansvarar för, vilka tekniska system som används samt vilka tekniska och kommunikationsmässiga krav som ställs av den aktuella nivån. Nedan följer en presentation av respektive nivå.



Figur 1. Lagerindelning för styrsystem.

2.1.1 Nivå 0 – Fältnivå

På den lägsta nivån finns processen, det vill säga den process som informations- och styrsystemet kontrollerar och övervakar. I större system såsom en fabrik motsvarar processen de steg i tillverkningen som är automatiserade från mottagning av råvaror eller komponenter till den sammansatta och leveransklara produkten. För distributionssystem fokuserar processnivån på distributionskedjan från producent till konsument, antingen hela kedjan eller en delmängd av den.

Fältnivån omfattar endast processen. Således ligger styrsystemet och dess sensorer och ställdon på högre nivåer i lagerindelningen.

2.1.2 Nivå 1 – Direktkontroll

På nivå 1 övervakas och styrs fältnivån genom sensorer och ställdon. Data från sensorer skickas till utrustning på nivå 2, samtidigt som styrinstruktioner till ställdon tas emot från den nivån.

På direktkontrollnivån återfinns sensorer och ställdon för att läsa av och påverka processen.

2.1.3 Nivå 2 – Produktionskontroll

Nivå 2 avser produktionskontroll. Det här är ofta den lägsta nivå där människor normalt hanterar styrsystemet under drift. Styrutrustning på nivå 2 kontrollerar sammanhängande men avgränsade delar av produktionsprocessen, med syftet att bevara kontroll och stabilitet i processen. På den här nivån kan flera processtyrningsmodeller vara aktuella, såsom för diskreta processer, batchprocesser och kontinuerliga processer.

Utrustning på nivå 2 är exempelvis programmerbara styrenheter (eng. *programmable logic controllers*, PLC) och datorundercentraler (DUC).

2.1.4 Nivå 3 – Produktionsledning

På nivå 3 koordineras personal, utrustning och material i syfte att optimera produktionen. Från nivå 3 sker den övergripande övervakningen och kontrollen av processen. För ett fabrikssystem styrs verksamheten genom planering och schemaläggning. I ett distributionssystem motsvarar denna nivå en central övervakningsplats. På den här nivån sker också kommunikation av produktionsmål och produktionsresultat med verksamhetsledningen på nivå 4.

På produktionsledningsnivån återfinns styr- och övervakningssystemet (eng. *supervisory control and data aquisition,* SCADA).

2.1.5 Nivå 4 – Verksamhetsledning

Den översta nivån avser affärsverksamhet. Den verksamhet som sker på nivå 4 påverkar eller påverkas av produktionssystemen, det vill säga nivå 1-3, men det sker inte någon direkt styrning av dessa nivåer. Påverkan är snarare indirekt, exempelvis genom uppföljning av produktionsekonomi eller styrning av vilka produkter som ska tillverkas.

På verksamhetsledningsnivån återfinns affärssystemen (eng. *enterprise resource planning*, ERP).

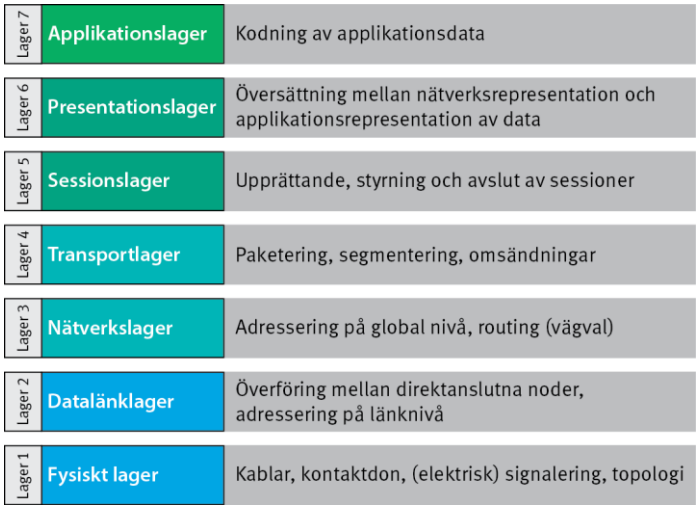
2.2 OSI-modellen

Open systems interconnection (OSI), vanligen benämnd OSI-modellen, är en universell beskrivningsmodell för protokollhierarkier inom elektronisk kommunikation som togs fram genom ett samarbete mellan ISO[1] och ITU-T[2] (ISO/IEC 1994).

OSI-modellen består av sju lager enligt figur 2. Det översta lagret ligger närmast applikationen och lagret längst ner motsvarar det fysiska medium som kommunikationen sker över.

Modellen bygger på att protokollen på respektive lager nyttjar tjänster som tillhandahålls av lagret under och att protokollen erbjuder tjänster till lagret över. I modellen sker all interaktion mellan näraliggande lager.

[1] International Organization for Standardization, http://www.iso.org [hämtad 2017-05-19]
[2] International Telecommunication Union, Telecommunications standardization sector, http://www.itu.int/en/ITU-T [hämtad 2017-05-19]



Figur 2. OSI-modellens sju lager.

En viktig aspekt när det gäller förståelsen av OSI-modellen är att alla lager inte alltid är relevanta. Många protokoll inkluderar inte vissa lager då funktionaliteten i de lagren inte behövs. Till exempel så saknas sessionslagret i många av de enklare protokollen för industriella informations- och styrsystem då dessa baseras på enkla frågor och svar där det inte finns någon anledning att hålla koll på aktuellt tillstånd för kommunikationen. I dessa fall kan sessionsfunktionaliteten ses som något manuellt, där en människa har konfigurerat samt anslutit enheterna och därmed kopplat upp sessionen.

I diskussionen om protokollstrukturer är det viktigt att skilja på protokoll och protokollager. Ett protokoll kan mycket väl definiera funktionen som motsvarar flera protokollager, något som också är mycket vanligt. Protokollagren innebär en principiell indelning, från fysisk nivå till applikationsnivå, medan protokollen snarare är en funktionsdriven indelning, baserad på vad den som designar protokollet vill få ut för funktioner.

I vissa fall skapas protokoll som direkt passar in på ett enda protokollager, dock tenderar dessa protokoll att vara breda i sitt användningsområde där fokus ofta ligger på att stödja ett flertal över- och underliggande protokoll. Protokoll avsedda för industriella informations- och styrsystem har i regel ett tydligt och avgränsat användningsområde, med tydliga gränsytor mot andra protokoll, vilket gör att dessa ofta definieras utan direkt hänsyn till lagerindelningen.

2.2.1 Lager 1 – Fysiskt lager

Det fysiska lagret erbjuder en grundtjänst som i princip är överföring av bit-orienterad information mellan två eller flera fysiska entiteter.

Detta lager hanterar alla fysiska aspekter av kommunikationen. I detta ingår bland annat kablar, kontaktdon och elektrisk/optisk signalering för kabelbunden transmission samt frekvensband och modulering för radiotransmission.

2.2.2 Lager 2 – Datalänklager

Datalänklagret är det logiska lager som ligger närmast det fysiska lagret. I datalänklagret ingår adressering på lägsta nätverksnivå och överföring av data mellan fysiska entiteter.

2.2.3 Lager 3 – Nätverkslager

Nätverkslagret hanterar utbyte av data mellan de kommunicerande parterna över ett logiskt nätverk. Det logiska nätverket innehåller ofta någon form av adressering och detta lager svarar för att skicka vidare paket i ett routat nätverk.

2.2.4 Lager 4 – Transportlager

Transportlagret erbjuder ett antal tjänster för att överföra data mellan de kommunicerande parterna genom överliggande lager. Överföringen kan antingen vara förbindelseorienterat (eng. *connection oriented)* eller förbindelselöst (eng. *connectionless)*.

Ett protokoll som är förbindelseorienterat brukar ha ett flertal egenskaper som förenklar kommunikationen för ovanliggande lager. Grundegenskapen är att en kommunikationskanal upprätthålls mellan parterna av transportlagret så länge som kommunikation ska pågå. Ytterligare egenskaper i transportlagret kan vara flödeskontroll, bekräftad leverans av paket, automatiska omsändningar och garantier på att data levereras i samma ordning som de sändes.

I förbindelselösa protokoll utgör transportlagret i regel en enkel överföringsmekanism där paket skickas utan de extra funktioner som räknas upp för förbindelseorienterade protokoll.

2.2.5 Lager 5 – Sessionslager

Sessionslagret ansvarar för att skapa, upprätthålla och avsluta kommunikationssessioner mellan kommunicerande parter. En session kan ses som en avgränsad men sammanhängande dialog mellan parterna, där dessa kan utbyta information utan att behöva återupprepa meta-information såsom adressering eller kontext.

En session kan liknas vid ett telefonsamtal, som inleds med att ena parten ringer upp (uppkopplingsförfarande), följt av samtalet (informationsutbyte) och att parterna lägger på luren (nedkopplingsförfarande).

2.2.6 Lager 6 – Presentationslager

Presentationslagret innehåller översättningsfunktioner för att koda om information från applikationslagret till ett format som lämpar sig för vidare hantering i lägre lager. En typisk funktion på detta lager är att serialisera applikationens interna datarepresentation så att den kan överföras som en sekvens av tecken.

2.2.7 Lager 7 – Applikationslager

Applikationslagret ligger närmast användarapplikationen och kapslar in den applikationsspecifika kommunikationen. Detta lager interagerar med funktionerna i applikationen och därmed finns inget högre lager i protokollstacken.

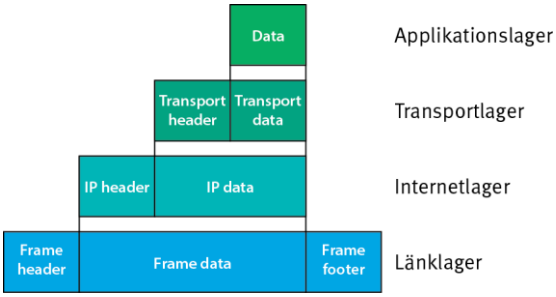
Applikationslagret innehåller ofta funktionalitet för att bland annat identifiera kommunikationspartner och ta reda på vilka resurser som finns tillgängliga för kommunikationen. En annan funktion som ofta ligger i detta lager är autentisering och auktorisering av kommunicerande parter.

Det är viktigt att särskilja applikationslagret och applikationen. Applikationen, som faller utanför OSI-modellens lagerstruktur, innehåller i regel betydligt mer funktionalitet än applikationslagrets protokoll, även om applikationslagret ofta implementeras direkt i applikationen.

2.3 Internetprotokoll-modellen

OSI-modellen är endast en av ett flertal lagerindelningar för protokollstackar i datornätverk. En av de vanligaste modellerna är den som används för beskrivning av sviten av *internetprotokoll*[3], en svit som ofta refereras till som TCP/IP-protokollen (IETF 1989). Denna modell har endast fyra protokollager, nämligen applikationslager, transportlager, internetlager och länklager[4].

[3] IETF (1989) använder namnet *Internet protocol suite* för samlingen av internetprotokoll.
[4] Eng. *application layer*, *transport layer*, *internet layer* och *link layer*.



Figur 3. TCP/IP-modellen.

Figur 3 visar TCP/IP-modellens lagerindelning och förenklat hur dessa kapslar in överliggande lagers data. Applikationslagrets protokoll specificeras inte i internetprotokollsviten då detta lager innehåller många protokoll med olika egenskaper. Exempel på ett applikationsprotokoll inom industriella informations- och styrsystem är *Modbus TCP* som ligger ovanpå internetprotokollen.

Internetprotokollsviten innehåller två transportprotokoll, *user datagram protocol* (UDP) och *transmission control protocol* (TCP), med olika egenskaper. UDP är ett enkelt protokoll där paketen skickas utan några som helst garantier på att dessa når mottagaren. TCP är däremot anslutningsorienterat och innehåller bland annat stöd för flödeskontroll och att paket levereras till överliggande lager hos mottagaren i rätt ordning. TCP är det dominerande transportprotokollet på internet.

Internetlagret omfattar *internet protocol* (IP) samt två stödprotokoll. IP är det fundamentala protokollet på internet och innehåller bland annat stöd för global adressering. IP finns i två versioner, IPv4 och IPv6, med olika modeller för adressering, där IPv4 är kraftigt dominerande idag. En av de viktigaste skillnaderna mellan IPv4 och IPv6 är att det senare kan adressera många fler enheter, något som börjar få allt större relevans på internet idag. Inom industriella kontroll- och styrsystem är begränsningen i antal adresser som IPv4 kan hantera normalt sett inget problem då systemen inte bör vara direktkopplade till internet.

Länklagret utgör den nivå som överför IP-paket på ett fysiskt medium, inklusive den fysiska adresseringen som krävs på den nivån. Länklagrets protokoll är inte direkt specificerade inom internetprotokollsviten, men ett vanligt val på länklagernivån är Ethernet.

Det finns ingen direkt korrespondens mellan lagerindelningen i OSI-modellen och den i internetprotokollsviten. Detta beror delvis på att OSI-modellen är striktare än internetprotokollsviten i uppdelningen av lagren och att internetprotokollsviten är mer fokuserad på en praktisk implementation, snarare än att vara en universell förklaringsmodell.

3 Metod

Studien har genomförts i två steg, först en intervjuserie för att utröna vilka protokoll som förekommer i industriella informations- och styrsystem inom samhällskritisk infrastruktur, följt av en litteraturgenomgång fokuserad på att samla in information om dessa protokoll.

3.1 Intervjuer

Syftet med intervjuerna är att få en bild av vilka protokoll som oftast förekommer i svenska installationer inom kritisk infrastruktur. Informationen som samlats in i intervjuerna utgör underlag för det protokollurval som har gjorts vid litteraturgenomgången.

3.1.1 Urval av respondenter

Respondenterna har valts ut så att de ger en relativt bred täckning inom kritisk infrastruktur. Respondenter har sökts inom följande verksamhetsområden:

- Rening och distribution av dricksvatten samt omhändertagande och rening av avlopp.
- Elproduktion (vattenkraft och kärnkraft) samt eldistribution.
- Fjärrvärmeproduktion och fjärrvärmedistribution.
- Spårbunden trafik.

När lämpliga personer har identifierats har dessa kontaktats för att undersöka möjligheten att få genomföra en intervju. Genom detta förfarande har forskarna nått respondenter inom samtliga verksamhetsområden förutom spårbunden trafik, där de tillfrågade personerna tyvärr inte har haft möjlighet att ställa upp på en intervju under den period som studien genomfördes.

3.1.2 Genomförande

Intervjuerna leddes av två personer från FOI och genomfördes via telefon eller på plats hos respondenterna i de fall där det varit praktiskt möjligt. Normalt sett utfördes intervjuer med en respondent åt gången, men i några fall deltog flera respondenter i samma intervju. I dessa fall kom samtliga respondenter från samma organisation och deltog huvudsakligen för att täcka in relevanta roller inom organisationen.

Intervjuerna har genomförts på följande sätt:

- Intervjun inleds genom att forskarna presenterar sig själva, projektet och syftet med intervjun samt ger tidsramen på ca 30–45 minuter för intervjun.
- Respondenten presenterar sig och sin roll samt har möjlighet att ställa eventuella frågor som denne har om intervjun.
- Forskarna intervjuar respondenten enligt en förberedd intervjuguide.
- Intervjun avslutas och respondenten ges möjlighet att ställa ytterligare frågor eller göra tillägg till det som sagts under intervjun.

Frågorna i intervjuguiden utgjorde endast ett stöd för att ge struktur och för att se till att alla områden har berörts under intervjun. Genom att upprätthålla målet att hinna igenom alla frågor i intervjuguiden inom avsatt tidsram fördes intervjun hela tiden framåt och risken att fastna för länge på enskilda frågor minskade, även om respondenten naturligtvis gavs utrymme att utveckla svar som bedömdes relevanta.

Intervjufrågor av allmän karaktär har under intervjuernas gång om möjligt konkretiserats för att bättre knyta an till respondentens roll och arbetsuppgifter. Beroende på respondentens roll var vissa frågor dessutom relevanta endast i vissa intervjuer.

3.2 Litteraturgenomgång

En översiktlig genomgång av tänkbara protokoll gjordes innan intervjuerna i förberedande syfte inför intervjutillfällena. Det primära arbetet med litteraturgenomgången har dock varit att skaffa sig fördjupad kunskap om de protokoll som är de mest nyttjade enligt intervjuerna. De specifikationer och annan dokumentation kring protokollen som varit möjliga att få tillgång till har samlats in och studerats för att utgöra underlag för protokollbeskrivningarna i rapporten.

4 Resultat

Det huvudsakliga målet med studien var att få en bild över vilka protokoll som används inom kritiskt infrastruktur samt inom vilka sektorer som protokollen förekommer. Dessa aspekter utgör de huvudsakliga forskningsfrågorna i studien.

Förutom att ta upp aspekter direkt relaterade till de huvudsakliga forskningsfrågorna i intervjuerna så ställdes även frågor om systemens övergripande uppbyggnad och varför systemen nyttjade de protokoll som används. Dessa frågor ses som relevanta för att förstå varför fördelningen av protokoll ser ut som den gör inom respektive sektor.

4.1 Protokollanvändning

Alla sektorer har en relativt spretig användning av protokoll inom industriella informations- och styrsystem, mycket beroende på att en stor andel av systemen innehåller delar med gammal utrustning vilket gör att äldre protokoll måste användas av kompatibilitetsskäl. Tabell 1 visar en översikt över de protokoll som tagits upp av respondenterna och inom vilka verksamhetsområden som de används.

Tabell 1. Översikt över protokollanvändning. X markerar protokoll som är vanligt förekommande, (X) markerar protokoll som används i mindre utsträckning.

Protokoll	Leverantör	VA	El	Fjärrvärme
Modbus	Öppet protokoll	X	X	X
PROFIBUS	Öppet protokoll	X	X	X
COMLI	ABB	X		X
OPC/OPC UA	Öppet protokoll	X	X	X
MMS	Öppet protokoll	X	X	X
Cactus ASCII	Cactus	X		X
PROFINET	Öppet protokoll		X	
MasterBus	ABB	X		X
Melsec	Mitsubishi	(X)		(X)
EXOline	Regin	(X)		
AquaCom	Flygt	(X)		(X)
IEC 60870-5-104	Öppet protokoll		X	

I flera fall har respondenterna tagit över befintliga system som då har infogats bland de system som respondenterna arbetar med, exempelvis genom företagsförvärv eller andra organisatoriska förändringar. Systemen har ofta lång livslängd och utbyte skulle vara kostsamt varför arvssystemen många gånger blir kvar under ett stort antal år. Detta gör att de flesta respondenter beskriver komplexa system som i regel är spretiga ur såväl utrustnings- som protokollperspektiv.

Det finns även en stor överensstämmelse mellan de protokoll som används inom VA och fjärrvärme. Detta beror sannolikt på att system inom dessa sektorer traditionellt sett ägts av samma aktörer, företrädesvis kommuner. På många håll har fjärrvärmeproduktionen sålts till privata aktörer, men dessa lever under överskådlig tid framöver med arvssystemen från den kommunala tiden och överensstämmelsen lär således fortsätta att vara hög mellan de två sektorerna.

4.2 Vad styr val av protokoll

Vid intervjuerna har frågor ställts kring hur valet av protokoll går till när en ny anläggning tas fram eller en befintlig anläggning uppgraderas. Här skiljer sig svaren beroende på om respondenten representerar en aktör närmare leverantörssidan, som av naturliga skäl förordar produkter som de själva tillverkar och säljer, eller om respondenten representerar systemägarna, där valet oftare styrs av den egna kunskapen och vad som finns i systemen sedan tidigare.

Utifrån intervjuerna går det att urskilja tre principer som styr vilka protokoll som väljs. Principerna baseras på i vilken grad systemägaren vill detaljstyra systemuppbyggnaden och på hur upphandling och inköp görs. De tre principerna är att

- upphandlingsregler styr
- beställaren ställer krav
- leverantören bestämmer.

4.2.1 Upphandlingsregler styr

I denna kategori styrs beställaren mer eller mindre av upphandlingsregler kring vilken eller vilka leverantörer som levererar och installerar utrustningen. Beställaren har i dessa fall inte så mycket att säga till om och till mångt och mycket bestämmer priset vilken lösning som levereras, vilket oftast leder till att den utpekade leverantören väljer vilka protokoll som används.

4.2.2 Beställaren ställer krav

Vissa beställare ställer krav på vilka protokoll som leverantören ska använda. För att detta ska vara möjligt krävs att kunnande finns inom beställarens organisation, för att kunna specificera hur lösningen ska utformas. Förutsättningar för detta kan vara att beställaren har en tillräckligt stor organisation med tillräcklig kompetens och resurser nog för att specificera vilka protokoll som ska nyttjas, alternativt att det inom organisationen har fastslagits en policy kring vilka protokoll som ska användas.

När det finns möjlighet att ställa krav på vilka protokoll som ska användas bygger valet typiskt på en av två principer:

- **Samma protokoll som tidigare** – Krav på kompatibilitet styr ofta i situationer där beställaren ställer krav på att utrustning från samma tillverkare som tidigare ska användas eller att utrustning som kan hantera samma protokoll som befintlig utrustning ska användas. Att integrera ny utrustning från samma leverantör med den befintliga utrustningen upplevs generellt sett som betydligt mindre komplicerat än att introducera andra tillverkares utrustning och att få den att fungera med övrig utrustning och protokoll som redan finns på plats.
- **Öppna protokoll** – Genom att kravställa att öppna och standardiserade protokoll ska användas blir lösningarna inte knutna till en viss leverantör och att denne måste utföra installation och underhållsarbete. En fördel med detta jämfört med att använda användarspecifika, proprietära protokoll är att system från olika leverantörer kan integreras.

  Ett problem som tagits upp av respondenterna med att kravställa öppna protokoll är att risken landar på systemägaren snarare än leverantören om det uppstår problem i integrationen.

4.2.3 Leverantören bestämmer

Denna situation var vanligast bland de aktörer vi intervjuade. Ofta föredrar de som levererar PLC:er och annan utrustning att arbeta med specifika protokoll. I vissa fall handlar det om att leverantören förordar sin utrustning och att leverantören tillhandahåller en helhetslösning inklusive tillverkarspecifika protokoll. I andra fall handlar det om att leverantören har erfarenhet sen tidigare av en viss tillverkares utrustning som därför ligger närmare till hands att förorda även till andra kunder.

5 Protokollbeskrivningar

Det finns många olika protokoll för industriella informations- och styrsystem och detta avsnitt tar upp de som har visat sig vara vanligast i svensk kritisk infrastruktur enligt intervjuresultaten. Flera av de protokoll som nämndes i intervjuerna tas inte upp i detta avsnitt då de användes sparsamt, ofta i ett enstaka, äldre styrsystem.

För vissa tillverkarspecifika protokoll har det varit svårt att hitta konkret information vilket har begränsat möjligheten att studera dem närmare. Det finns även protokoll med en mängd olika varianter, där det har visat sig vara svårt att få reda på exakt vilken variant av protokollet som används. Internt i organisationen är det inte ovanligt att egna benämningar blir vedertagna, något som gör att det inte är självklart vilket protokoll som avses. I vissa fall kan benämningen dessutom motsvara en rad olika varianter av ett protokoll. Exempelvis har vi stött på benämningen ”Mitsubishi-protokollet”, trots att Mitsubishi har en rad olika varianter av sina kommunikationsprotokoll. För aktörerna själva är detta inget problem då de själva vet vilket protokoll som avses, vilken protokollvariant och version som används är då underförstått. Detta gör att det blir en utmaning för en utomstående att identifiera exakt vilken specifikation som avses.

Många protokoll har funnits i flera decennier och har av naturliga skäl utvecklats vilket gör att det i många fall finns flera versioner av samma protokoll med tillhörande specifikationer. Vilken exakt version av protokollet som används har inte alltid varit känt av respondenten. Beskrivningarna som följer utgår om inget annat anges från den senaste versionen av specifikationerna.

Reservation görs för faktafel i protokollbeskrivningarna då den tillgängliga dokumentationen i vissa fall är otydlig, motsägande eller saknar information som behövs för beskrivningarna.

5.1 Förklaring av protokollbeskrivningar

Varje protokoll beskrivs i ett avsnitt och följer samma upplägg. Följande delar ingår i varje protokollbeskrivning:

- **Inledningen** av respektive avsnitt ger en kortfattad introduktion till protokollet och dess egenskaper.
- Avsnittet **varianter** tar upp de olika varianterna av protokollet som används eller har använts.
- Avsnittet **användningsområde** visar hur protokollet passar in i referensmodellen för styrsystem samt i OSI-modellen. Protokollspecifikationerna pekar i vissa fall ut standardprotokoll som ska

användas på underliggande OSI-lager. I dessa fall är de OSI-lager som hanteras genom standardprotokoll skrivna inom parentes.

- Avsnittet **datamodell** ger en kortfattad beskrivning av den datamodell som anges i protokollspecifikationerna. I de fall som datamodellen är komplex ges en övergripande förklaring till hur datamodellen avses att fungera och användas.
- Avsnittet **säkerhet** tar upp säkerhetsaspekter, avseende såväl drift-säkerhet som informations- och IT-säkerhet.
- Avsnittet **specifikationer** innehåller en förteckning av referenser till specifikationer som beskriver protokollet eller protokollfamiljen.

5.2 AquaCom

AquaCom är ett protokoll som primärt är avsett för styrning av vattenpumpar. Protokollet är framtaget av svenska ITT Flygt, numera en del av Xylem.

Anslutningen mellan ett centralt system och en RTU från Flygt använder sig av fast eller uppringd modemkommunikation, men det är även möjligt att använda en direktansluten seriell kommunikationskanal. Kommunikationen i AquaCom sker med meddelanden som benämns telegram. Dessa kan överföras över såväl uppringda som fasta förbindelser.

- **Uppringd förbindelse** – Vid användning av en uppringd kommunikationslinje kontaktar den centrala enheten en RTU när behov av kommunikation finns. RTU:n kontaktar bara centrala enheten när ett larm har inträffat.
- **Fast förbindelse** – När fast förbindelse används är det möjligt att använda flerpunktskommunikation (eng. multidrop) med flera RTU:er anslutna. Maximala antalet anslutna RTU:er beror på modemtillverkare samt längden och kvaliteten på förbindelsen. Dessa faktorer avgör även hur lång tid det tar att fråga alla RTU:er efter dess larmstatus. Som exempel anger specifikationen att maximala antalet enheter ligger på 5–10 RTU:er anslutna över en fast förbindelse upprättad med ett V.23-modem.

Specifikationen föreskriver att kommunikationen företrädesvis ska ske via V.23-modem, även om det förekommer andra modemtyper för vissa RTU:er.

Kommunikationen görs genom huvudsakligen läsbar ASCII, med teckenformatet 8 bitar, en stoppbit och ingen paritet, även om oläsbara specialtecken används för bland annat inramning (eng. *framing*) av telegrammen.

Adressering av RTU:er görs via identiteter som kallas ”logical plant number” för uppringda enheter och ”node ID” vid fast uppkoppling.

5.2.1 Varianter

Det finns endast en variant av AquaCom. Olika RTU:er stödjer olika uppsättningar av meddelanden (kommandon) som skickas via protokollet.

5.2.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager (2. Datalänklager) (1. Fysiskt lager)

5.2.3 Datamodell

Specifikationen för AquaCom beskriver ingen datamodell och det är svårt att läsa ut en tydlig datamodell ur de meddelanden som protokollet stödjer. Uppbyggnaden i protokollet bygger snarare på hur implementationerna ser ut i de RTU:er som protokollet togs fram för att stödja.

5.2.4 Säkerhet

Driftsäkerhet

En checksumma inkluderas i telegrammeddelandena och beräknas på telegrammets ingående tecken. Specifikationen föreskriver inte hur utrustningen förväntas hantera inkommande telegram med felaktig checksumma.

Vissa centrala enheter kräver även att RTU:n identifierar sig med en unik identifierare när den svarar på anrop. Denna identifiering är inte specifikt skyddad och utgör således ingen autentisering, däremot kan den skydda mot felaktiga anslutningar och felaktiga konfigurationer i ansluten utrustning.

Informationssäkerhet

AquaCom innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.2.5 Specifikationer

Technical description AquaCom – RTU level Rev 1.6. ITT Flygt AB 2004.

5.3 Cactus ASCII

Cactus ASCII är ett protokoll framtaget av företaget Cactus Utilities AB. Cactus egna SCADA-system Cactus Eye använder företrädesvis Cactus ASCII vid kommunikation med företagets egna understationer (PLC:er), även om Cactus Eye även kan använda ett flertal andra protokoll för att kunna kommunicera med utrustning från andra tillverkare.

När kommunikation sker i ett distribuerat system med Cactus ASCII finns följande alternativ att välja bland:

1. Centraldator direktkopplad till understation, det vill säga centraldatorn betjänar endast en understation via varje kommunikationskanal.
2. Centraldator kopplad till understationer med hjälp av multidrop, det vill säga en kanal på centraldatorn används för flera understationer.
3. Centraldator är kopplad till understationer över uppringd eller automatsvarande anslutning via telenätet. Kommunikation kan ske med flera understationer, dock bara med en understation i taget.
4. Centraldator direktkopplad till en koncentrator, ett slags sammankopplingsenhet, för vidare kommunikation ut mot flera understationer.

I samtliga fall sker kommunikationen i halv duplex och överföringar sker huvudsakligen i läsbar ASCII. Kodningen till läsbar ASCII innebär att underliggande binär data kodas så att en byte data representeras med två ASCII-tecken, motsvarande de hexadecimala strängarna ”00”–”FF”. Viss utrustning klarar av kommunikation i binärt format och då behövs inte översättningen till hexadecimalt.

All kommunikation över Cactus ASCII bygger på att servern frågar dess anslutna understationer efter information och att denna i sin tur svarar. Protokollet består huvudsakligen av tre olika typer av meddelanden: pollning, datameddelanden och kvittenser.

Pollning

Pollning sker genom att centraldatorn skickar identiteten på den understation den vill kommunicera med. Svarsalternativen till centraldatorn är:

- Identiteten på understationen, vilket indikerar att data saknas.
- Datameddelande (enligt nedan).
- Timeout eller ogiltigt meddelande.

Datameddelande

Datameddelande som skickas innehåller identitet, meddelandetyp, data och checksumma. Identitet, meddelandetyp och checksumma utgör 1 byte var medan datafältet kan vara på maximalt 294 bytes.

Kvittens

Alla meddelanden som skickas kvitteras alltid med ett meddelande som består av ett utropstecken (’!’) när korrekt checksumma mottagits. Om centraldatorn tar emot ett felaktigt tecken eller om timeout inträffar ska omsändning alltid ske. För att indikera att en omsändning önskas bör understationen skicka ett frågetecken (’?’).

5.3.1 Varianter

Cactus ASCII finns endast i en variant som inkluderar de variationer som förekommer i protokollet och dess användning.

5.3.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager

5.3.3 Datamodell

Datamodellen som presenteras i specifikationen består av femton tabeller. Tabellerna omfattar in- och utgångar för såväl logiska som analoga värden samt tabeller för automatisk in- och utrapportering av förändringar. Dessutom finns ytterligare tabeller för lokal användning samt för timers.

5.3.4 Säkerhet

Driftsäkerhet

Protokollet använder sig av en checksumma för att säkerställa att meddelanden som skickas överförts korrekt.

Informationssäkerhet

Cactus ASCII innehåller inga specifika säkerhetsmekanismer för informations-säkerhet.

5.3.5 Specifikationer

Kommunikation med Cactus ASCII, System CSX Version 8.0. Cactus Utilities AB.

5.4 COMLI

COMLI, kort för Communication Link, är ett protokoll som ursprungligen togs fram av SattControl, sedermera uppköpt av ABB Automations Control System. COMLI har under årens lopp utvecklats för att stödja nya system samtidigt som stöd för vissa äldre system delvis har tagits bort. ABB rekommenderar därför att integratören studerar såväl specifikationen för COMLI som de enskilda systemens stöd för COMLI.

Kommunikationen i COMLI är uppbyggt som ett enkelt nätverk med en master och en eller flera slavar. Kommunikationen sker seriellt i halv duplex. System med en slav kan nyttja RS-232, RS-485 eller strömslinga för det fysiska lagret. Om COMLI ska användas för att kommunicera med flera slavar används RS-485.

COMLI är meddelandebaserat protokoll som definierar ca 50 meddelandetyper beroende på protokollversion. Dessa meddelanden kan delas in i tre typer:

- Förfrågningar (eng. requests) från master till slav.
- Dataöverföring från master till slav eller slav till master.
- Bekräftelsemeddelande (eng. acknowledge message, Ack) från slav till master.

5.4.1 Varianter

Det finns endast en variant av COMLI.

5.4.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager (2. Datalänklager) (1. Fysiskt lager)

5.4.3 Datamodell

Specifikationen för COMLI beskriver ingen datamodell. De meddelanden som ingår i protokollet ger möjlighet att läsa och skriva bland annat digitala I/O-signaler, analoga I/O-signaler, digitala register, larm, datum/tid, flyttalsregister och minnesutrymme.

Överföring av minnesutrymmet är uttryckligen till för att smidigt kunna sköta säkerhetskopiering av utrustningen till master-datorn. Meddelanden finns för att såväl läsa som skriva minnesutrymmet i utrustningen.

5.4.4 Säkerhet

Driftsäkerhet

COMLI har följande egenskaper för att säkerställa att överföringen lyckats:

- En checksumma (Block Check Count, BCC) beräknat på meddelandets innehåll.
- Paritet på överförda bytes för att detektera transmissionsfel.
- Slav-enheten ger fel om meddelandet den tar emot inte hanteras.
- Ett COMLI-meddelande innehåller även en märkning, STAMP, som indikerar om ett meddelande skickas för första gången eller om det utgör en omsändning. Denna märkning är till för att undvika att samma meddelande processas flera gånger av enheten.

Informationssäkerhet

COMLI innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.4.5 Specifikationer

COMLI System Description. ABB Satt AB. 1998.

5.5 EXOline

EXOline är ett protokoll framtaget av Regin Exomatic AB och används bland annat för att kommunicera med RTU:er och andra kontrollenheter från Regin Exomatic AB, även benämnda *moduler*.

Protokollet är uppbyggt med en master och en eller flera slavar, där master alltid initierar kommunikationen. Alla meddelanden från mastern efterföljs av ett svar från den adresserade slaven om inte kommunikationsfel uppstår. Först efter att svaret mottagits eller en timeout har skett kan ett nytt kommando skickas.

Innan en modul svarar så kan den skicka så kallade stopptecken (eng. wait characters) för att indikera att den är upptagen med att behandla kommandot. Stopptecknen möjliggör kort timeout och bra anpassning till olika långa fördröjningar i kommunikationskanalen utan att sätta onödigt höga krav på tiden det tar att hantera kommandon hos slavarna.

Om en slav inte tar emot ett komplett meddelande eller om det sker en timeout så svarar den inte. Om en master inte får ett komplett meddelande eller det sker en timeout så skickar den meddelandet på nytt.

Protokollet är byte-orienterat och meddelandena som skickas är endera ett kommando till eller svar från en modul. Längden på ett meddelande är på maximalt 256 bytes, men specifikationen noterar att meddelanden i regel är betydligt mindre.

Escape-ersättning

Innan ett meddelande skickas görs escape-ersättning. Det innebär att alla förekomster av start-/sluttecken eller escape-tecken i meddelandet ersätts med ett escape-tecken (”1B” hexadecimalt) samt det faktiska tecknet inverterat för att undvika tvetydighet. När ett meddelande sen tas emot görs omvändningen för att återfå det ursprungliga meddelandet.

5.5.1 Varianter

EXOline-protokollet finns i två olika varianter, ett för seriell överföring och en för nätverksströmmar över TCP. Protokollet är i huvudsak detsamma oavsett transmissionsmedium.

EXOline – Seriellt

Över seriella länkar, exempelvis RS-232 och RS-485, är transmissionsformatet 8 bitar data med udda paritet och en stoppbit. EXOline-protokollet är designat att klara kommunikation över multidrop-länkar såsom RS-485.

Kommunikation över modem och andra typer av mediekonverterare stödjs av protokollet, även om specifikationen uttryckligen pekar på ett antal fallgropar med sådan teknik som integratörer och användare måste vara medvetna om.

EXOline – TCP

Vid överföring via TCP/IP kan en master kommunicera med multipla slavar på samma fysiska medium. Det är även möjligt för en dator att implementera flera EXOline-masters som var och en kommunicerar med flera slavar över samma medium.

Protokollspecifikationen förutsätter att TCP-anslutningar kopplas ner efter relativt kort tid. I ytterlighetsfallet kopplas TCP-anslutningen upp för varje kommando/svar-transaktion men då detta ger ganska hög trafikoverhead föreslås en timeout på c:a två minuter efter senaste meddelandet innan anslutningen kopplas ner.

För kommunikation via EXOline TCP skickas inte stopptecken (eng. *wait characters*) för att undvika timeouts. Fel, exempelvis ”inget svar”, indikeras genom att den sida som upptäcker problemet stänger TCP-anslutningen. När andra sidan sedan upptäcker att TCP-anslutningen stängts ner ansvarar den för att avsluta TCP-sessionen korrekt på sin sida.

5.5.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager (4. Transportlager [TCP]) (2. Datalänklager [seriellt]) (1. Fysiskt lager [seriellt])

5.5.3 Datamodell

Det finns ingen uttrycklig datamodell beskriven i protokollspecifikationen. I kommandouppsättningen finns det bland annat kommandon för att läsa och skriva värden samt för att läsa, skriva och avlusa program som köra på modulerna.

5.5.4 Säkerhet

Driftsäkerhet

EXOline-meddelanden innehåller en checksumma som beräknas med hjälp av XOR på ingående tecken i meddelandet.

Svarsmeddelanden i EXOline innehåller ingen märkning som anger vilket meddelande det svarar på. Det kan skapa problem med att det inte går att veta vilket meddelande ett svar hör till om det anländer sent. Det är upp till implementationen av protokollet att ta hand om detta problem.

Vid implementation av EXOline TCP är det avgörande hur hanteringen av TCP-anslutningen implementeras. I och med att fel indikeras genom att TCP-förbindelsen bryts kan det innebära långa väntetider för att koppla upp förbindelsen på nytt om det görs på ett ineffektivt sätt.

Informationssäkerhet

Det finns inga specifika skyddsmekanismer i protokollet för informationssäkerhet. Specifikationen varnar uttryckligen för att EXOline TCP inte är ett säkert protokoll och att detta måste hanteras utanför protokollet vid behov, exempelvis genom VPN-anslutning.

5.5.5 Specifikationer

The EXOline Protocol. Regin Exomatic AB. 2003.

5.6 IEC 60870-5-104

IEC 60870-5 är en uppsättning standarder som beskriver en protokollsvit för kommunikation mellan styrsystem för anläggningar inom eldistribution. Protokollsviten definierades ursprungligen för seriella länkar, företrädesvis över uppringda eller fasta anslutningar i telenätet, men har genom tillägget IEC 60870-5-104 även specificerats med TCP/IP-nätverk som bärare.

IEC 60870-5 definierar många datatyper, såväl generella som varianter med speciella egenskaper som direkt avspeglar funktionalitet inom eldistribution.

5.6.1 Varianter

Det finns endast en variant av IEC 60870-5-104. Standarden kan ses som en variant inom IEC 60870-5, där andra varianter är exempelvis IEC 60870-5-101 som beskriver samma grundprotokoll över seriella kanaler.

5.6.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager

5.6.3 Datamodell

IEC 60870 specificerar ingen egen datamodell utan tillhandahåller endast funktionalitet för att överföra data av olika datatyper. Standarden tillåter mappning mot olika datamodeller, exempelvis IEC 61850 som är en standard för kommunikation mellan styrsystem inom eldistribution och specificerar en standarddatamodell. Understandarden IEC 61850-80-1:2016 utgör en guide för hur en översättning av datamodellen kan göras till kommunikationsformaten i IEC 60870-5-101/104.

Datamodellen i IEC 61850 bygger på logiska noder (eng. *logical nodes*, LN), logiska enheter (eng. *logical devices*, LD) och gemensamma dataklasser (eng. *common data classes*, CDC).

5.6.4 Säkerhet

Driftsäkerhet

IEC 60870-5-104 specificerar inga direkta driftsäkerhetsmekanismer förutom det som erbjuds av det underliggande transportlagret, exempelvis felupptäckt och omsändningar som hanteras genom TCP-lagret.

Informationssäkerhet

IEC 60870-5-104 har i sig inga specifika säkerhetsmekanismer för informationssäkerhet.

Standarden IEC 60870-5-7, som publicerades 2013, specificerar hur autentisering ska genomföras av meddelanden som skickas över protokollen IEC 60870-5-101 och -104. Förutom autentisering av meddelanden så krävs även att utrustningen ska skydda kommunikationen med TLS och certifikat för att uppfylla IEC 60870-5-7.

5.6.5 Specifikationer

Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles. IEC 60870-5-104. IEC 2006.

Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks. IEC 60870-5-101. IEC 2003.

Telecontrol equipment and systems – Part 5: Transmission protocols – Section 5: Basic application functions. IEC 60870-5-5. IEC 1995.

Telecontrol equipment and systems – Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351). IEC 60870-5-7, IEC 2013.

5.7 MasterNet (MasterBus 300)

MasterNet är en svit av relaterade protokoll som togs fram för kommunikation mellan servrar och utrustning i ABB:s Advant OCS-system. I sviten ingår flera protokoll, däribland MasterBus 300.

MasterBus 300 använder 10 Mbit/s Ethernet för de lägsta protokollagren och IEEE 802.2, *Link Layer Control* (IEEE 1998), för datalänklagret. Systemet kan byggas med koaxialkabel enligt den äldre Ethernet-standarden IEEE802.3-1985 (IEEE 1985) eller som ett modernare stjärnnät med repeatrar eller switchar. Om MasterBus-systemet byggs som stjärnnät i industriella miljöer förespråkas att optisk fiber används för att klara av miljön.

Specifikationen tillåter inte att Ethernet-infrastrukturen delas mellan MasterBus-systemet och andra funktioner, exempelvis för att koppla samman vanliga datorer. Ett MasterBus 300-nätverk kan ha maximalt 45 noder anslutna.

Protokollet är konstruerat för kommunikationsnät upp till 10Mbit/s (kategori 5 enligt IEEE 802.3) men tack vare en dynamisk återsändningstimer har protokollet inget problem att anpassa sig till lägre överföringshastigheter.

5.7.1 Varianter

Förutom MasterBus 300 så inkluderar MasterNet tre varianter av protokollet:

- **MasterBus 300E** – E:et i MasterBus 300E står för Extended. Protokollet är avsett för kommunikation över synkron seriell förbindelse i halv duplex, där längre avstånd stödjs än för vanliga 300-varianten av protokollet. I och med att MasterBus 300-protokollet är Ethernetbaserat och idag i större utsträckning körs över fiberoptik istället för koaxialnät har 300E delvis spelat ut sin roll.
- **MasterBus 300F** – Dokumentation från ABB nämner en variant av protokollet som heter MasterBus 300F. Ingen ytterligare information har gått att få tag på om detta.
- **MasterBus 200** – MasterBus 200 är ett äldre protokoll som bygger på seriell synkron överföring via RS-422. Protokollet beskrivs inte vidare här då MasterBus 300-familjen introducerades i mitten av 1980-talet och antas ha ersatt MasterBus 200.

5.7.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	5. Sessionslager 4. Transportlager 3. Nätverkslager (2. Datalänklager) (1. Fysiskt lager)

5.7.3 Datamodell

MasterNet-sviten beskriver inte applikationslagret och innehåller därmed ingen datamodell.

I AC 800M-systemet kan data skickas över MasterBus 300, även om MMS-protokollet förespråkas i första hand. Om MasterBus 300 används skickas data i form av så kallade DataSet som består av en adressdel och upp till 24 element (32-bits värden). Varje element kan utgöras av

- ett 16- eller 32-bitars heltal
- ett flyttal (eng real)
- 32 st binära värden.

Adressdelen består av en nätverksnod, avsändarens nätverksnummer och DataSet-identiteten.

5.7.4 Säkerhet

Driftsäkerhet

Det underliggande Ethernet-lagret innehåller funktioner för upptäckt av kollisioner samt återsändning av ramar. Ethernet-lagret innehåller även en checksumma för upptäckt av överföringsfel.

Informationssäkerhet

MasterNet-sviten innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.7.5 Specifikationer

MasterNet User's Guide. ABB dokumentnummer 3BSE 003 839R301. 2001.

5.8 MELSEC Communication (MC) protocol

Protokollet MELSEC Communication (MC) protocol är ett protokoll framtaget av Mitsubishi avsett för att kommunicera mellan PLC:er av typen MELSEC och andra externa enheter såsom datorer och lokala användargränssnitt (HMI, eng. *human machine interface*).

Protokollet kan kommunicera över MELSECNET som är en familj av seriella förbindelser eller över Ethernet. Valet av kommunikationsmedium är beroende på vilken variant av protokollet som implementeras och vilken utrustning som ska anslutas.

Protokollet inkluderar funktioner för att läsa och skriva värden (exempelvis I/O-status), etiketter (eng. *labels*, namn på variabler, in-/utgångar etc.), buffertminne och filer. Dessutom finns funktioner för att styra programflödet för att kunna avlusa program i PLC:er.

Meddelandeformatet skiljer sig åt beroende på vilken utrustning som är ansluten till nätverket. För seriell kommunikation finns det fem olika meddelandeformat, varav fyra använder ASCII och den femte använder binärt kodning. För kommunikation över Ethernet finns tre meddelandeformat som alla kan använda såväl ASCII som binär kodning. Användning av binärt format innebär i praktiken att ungefär halva datamängden krävs vid överföring.

5.8.1 Varianter

Det finns flera olika typer av transmissionsmedia för MELSEC-protokollet:

- **MELSECNET** – Optisk anslutning eller elektrisk anslutning över koaxialkabel. Optisk anslutning görs i form av en loop där alla enheter ansluts. Koaxialkabel ansluts linjärt och termineras i ändarna. Hastighet 1,25 Mbit/s.
- **MELSECNET/B** – Elektrisk anslutning över tvinnade par. Anslutningen görs så att alla enheter sitter i ett ringnät med två par för kommunikation i båda riktningarna. Hastighet upp till 1 Mbit/s.
- **MELSECNET/10** – Optisk anslutning eller elektrisk anslutning via koaxialkabel. Optisk anslutning görs i form av ett ringnät där alla enheter ansluts. Koaxialkabel ansluts linjärt och termineras i ändarna. Hastighet upp till 10 Mbit/s.
- **MELSECNET/H** – Optisk anslutning eller elektrisk anslutning via koaxialkabel eller tvinnat par. Optisk anslutning görs i form av en loop där alla enheter ansluts. Koaxialkabel och tvinnat par ansluts som ett bussnät och termineras i ändarna. Hastigheten kan vara upp till 25 Mbit/s på optisk fiber och upp till 10 Mbit/s för övriga media.

MELSECNET/H över tvinnat par har tagits fram för att kunna återanvända kablage vid uppgradering från tidigare MELSECNET/B-installationer.

- **Ethernet** – Anslutning via Ethernet, typiskt 10 eller 100 Mbit/s.

Det övergripande protokollet är detsamma oavsett transmissionsmedium, även om vissa kommandon bara är tillgängliga på vissa medium.

5.8.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager 5. Sessionslager 4. Transportlager 3. Nätverkslager (2. Datalänklager) (1. Fysisk lager)

5.8.3 Datamodell

MC-protokollet beskriver inte någon uttrycklig datamodell utan specificerar endast en uppsättning funktioner och kommandon för att utbyta data samt för att läsa, skriva och avlusa program som köra på enheterna.

5.8.4 Säkerhet

Driftsäkerhet

För alla meddelandeformat används checksumma för att säkerställa att informationen överförs korrekt.

När fler än en felkod uppkommer i ansluten utrustning returneras bara första felkoden som hittas vilket skulle kunna innebära problem om felkoder missas.

Informationssäkerhet

MELSEC Communication Protocol och MELSECNET innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.8.5 Specifikationer

MELSEC Communication Protocol Reference Manual. SH(NA)-080008-W. Mitsubishi Electric Corp.

Type MELSECNET, MELSECNET/B Data Link System Reference Manual. IB(NA)66350-G. Mitsubishi Electric Corp.

MELSECNET/10 Network Module User's Manual. IB(NA)-0800119-E. Mitsubishi Electric Corp.

MELSECNET/H Network Module User's Manual. IB(NA)-0800144-B. Mitsubishi Electric Corp.

5.9 MMS

Manufacturing Message Specification (MMS) är ett server-klient-baserat protokoll avsett för datoriserad tillverkningsindustri specificerad i den internationella standarden ISO/IEC 9506 sedan 1990. Protokollet utgör applikationslagret enligt OSI-modellen och syftar till att specificera kommunikation mellan programmerbara enheter.

Standarden består av två delar, där del 1 innehåller specifikationer på de tjänster som MMS tillhandahåller och del 2 innehåller protokollspecifikationen.

Protokollspecifikationen inkluderar hur meddelanden ska utbytas mellan MMS-noder, formatet för meddelanden samt definitionen av hur MMS ska interagera med andra OSI-lager. I specifikationen ingår:

- Standardobjekt som måste tillhandahållas av alla enheter. Detta hanteras genom en virtual manufacturing device (VMD).
- Standardmeddelanden som alla enheter måste stödja.
- Regler för hur meddelanden och data ska kodas.

Specifikationen av MMS-meddelanden i del två nyttjar standarden Abstract Syntax Notation Number One (ASN.1) för att specificera formatet (ISO/IEC 2015).

Virtual manufacturing device

Ett system anslutet till en MMS-miljö och som ska agera som server måste ha minst en *virtual manufacturing device* (VMD). En VMD är en abstrakt representation av tillverkningsutrustning innehållandes resurser och funktionalitet. VMD:n beskriver mappning till den underliggande funktionaliteten så att andra klientenheter i MMS-miljön kan kommunicera med denna.

Om en server exponerar mer än en VMD krävs att åtkomst till underliggande resurser koordineras vilket görs med så kallade semaforer i MMS. Semaforer används för att ge anropande klienter exklusiv åtkomst till en resurs i en VMD i taget.

Kortfattat innehåller en VMD

- objekt/variabler som servern exponerar
- tjänster som servern erbjuder för att påverka objekten
- effekten på servern när en klient använder tjänsterna.

5.9.1 Varianter

MMS har definierats i två varianter där den ursprungliga bygger på olika ISO-protokoll över Ethernet. Den nyare varianten använder TCP/IP över Ethernet. Tabell 2 visar en översikt över hur MMS nyttjar underliggande protokoll.

Tabell 2. Förenklad översikt över protokollager för MMS.

Lager	**Ursprunglig**	**Förenklad**
Applikationslager	MMS	
Presentationslager	ISO 8822/8823	
Sessionslager	ISO 8326/8327	
Transportlager	ISO 8072/8073	TCP, RFC 1006
Nätverkslager	ISO 8348	IP, ICMP
Datalänklager	Ethernet	
Fysiskt lager	Ethernet	

5.9.2 Användningsområde

Primär modellnivå	2. Produktionskontroll
OSI-lager	7. Applikationslager

5.9.3 Datamodell

MMS är ett objektbaserat protokoll med en mängd olika objektklasser, exempelvis namngivna variabler, semaforer och domäner, samt instanser och metoder som kan användas på objekten. Metoder benämns även *services* och kan inkludera sådant som läs, skriv och ladda ner.

MMS-objekt refereras normalt med hjälp av ett namn och kan tillhöra en av tre olika åtkomstrymder (eng. *scope*) inom vilket namnet ska vara unikt. Dessa åtkomstrymder är:

- VMD-definierad – Innebär att alla applikationer (anslutningar) till en VMD kan komma åt dessa objekt. Objekt består även efter att MMS-applikationen med VMD:n avslutas.
- Domän-definierad – Innebär att objekt är åtkomliga inom en domän. Domänen motsvarar en viss namngiven minnesrymd innehållandes program, variabler och data inom en VMD.

- Applikations-definierad – Innebär att objekt är åtkomliga endast inom en anslutning till en VMD. När MMS-applikationen avslutas försvinner också MMS-objektet.

5.9.4 Säkerhet

Driftsäkerhet

MMS förlitar sig på lägre protokollager för att hantera upptäckt av transmissionsfel, omsändningar och liknande. MMS beskriver i viss utsträckning hur kommunikationsfel ska hanteras i såväl protokollet som applikationen.

Informationssäkerhet

Specifikationerna för MMS fokuserar inte på säkerhetsaspekter, men anger att när särskilda säkerhetsaspekter behöver beaktas rekommenderas att detta görs utifrån den internationella standarden för OSI:s säkerhetsarkitektur (ISO/IEC 1989).

5.9.5 Specifikationer

Industriautomation – Specifikation av meddelande för produktionsutrustningar (MMS) – Del 1: Definition av tjänster. SS-ISO 9506-1, Utgåva 3. ISO.

Industriautomation – Specifikation av meddelande för produktionsutrustningar (MMS) – Del 2: Protokollspecifikation. SS-ISO 9506-1, Utgåva 3. ISO.

5.10 Modbus

Modbus är ett fältbussprotokoll som ursprungligen togs fram av företaget Modicon år 1979. Protokollet togs fram för överföring av data, exempelvis styrsignaler och mätvärden, över seriella kanaler mellan företagets PLC:er.

Modbus-kommunikation utgörs av transaktioner där en förfrågan (eng. *request*) från en master till en slav besvaras med ett svar (eng. *response*). En transaktion är antingen en skrivning eller en läsning. Datamodellen är en enkel och baseras på en abstraktion där alla ingångar och utgångar ses som oberoende, enskilda styrsignaler.

På 2000-talet togs en guide fram över hur Modbus-meddelanden kan skickas via TCP/IP. Senare har en integrerad specifikation tagits fram där applikationslagret inklusive kodning av meddelanden har separerats från de underliggande bärarnäten. Denna version av specifikationen tar upp TCP/IP, HDLC samt seriellt via RS-232/RS-485 som bärarnät. HDLC, *High-level Data Link Control*, är ett äldre protokoll för kommunikation över seriella transmissionskanaler.

Då Modbus är ett strikt master-slav-system finns ingen inbyggd möjlighet för slav-sidan att uppmärksamma en master vid en händelse, exempelvis ett larm. I de fall där snabb respons krävs för händelser så måste detta skötas utanför protokollet.

5.10.1 Varianter

I den senaste specifikationen förekommer endast en variant av Modbus och denna beskriver då applikationslagret, oavsett vilket bärarnät som används. I tidigare specifikationer finns dessa varianter:

- **Modbus-ASCII** – Direkt läsbar kodning (ASCII) av informationen, förmedlat via seriellt gränssnitt. Denna variant är inte med i nyare specifikationer men finns med i versionen från 1996.
- **Modbus-RTU** – Binär kodning av informationen, förmedlat via seriellt gränssnitt.
- **Modbus-TCP** – Samma kodning som i Modbus-RTU men förmedlat via TCP/IP.

5.10.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager (4. Transportlager [TCP/HDLC]) (2. Datalänklager [seriellt]) (1. Fysiskt lager [seriellt])

5.10.3 Datamodell

En transaktion i Modbus består av en förfrågan (*request*) och ett svar (*response*). Förenklat går det att säga att en förfrågan innehåller en funktionskod, en adress och eventuell data. Svaret på en lyckad transaktion innehåller samma funktionskod samt eventuell svarsdata. Vid en misslyckad transaktion består svaret av en felindikation samt en felkod.

Datamodellen för Modbus baseras på fyra tabeller enligt beskrivningen i tabell 3. Vilken tabell som en transaktion berör bestäms av de funktionskoder som används i förfrågan.

Modbus-specifikationen lägger ingen specifik tolkning av de fyra tabellernas innehåll. Den faktiska tolkningen av tabellinnehållet bestäms av tillverkaren till respektive produkt som implementerar Modbus.

De enda datatyperna som används i specifikation är binära värden och 16-bitarstal. Om funktionen i en produkt kräver andra datatyper måste dessa skapas genom en tolkning av information som överförs genom de två givna datatyperna.

Tabell 3. Datamodell för Modbus

Tabell	Format	Åtkomst	Användning
Discretes input	Bit	Läsning	Fysiska ingångar
Coils	Bit	Läsning Skrivning	Fysiska utgångar
Input registers	16-bit	Läsning	Interna register eller ingångsregister
Holding registers	16-bit	Läsning Skrivning	Interna register eller utgångsregister

5.10.4 Säkerhet

Driftsäkerhet

Modbus-ASCII och Modbus-RTU stödjer upptäckt av transmissionsfel genom checksummor medan Modbus-TCP förlitar sig på de underliggande protokoll-lagren för upptäckt och hantering av överföringsfel.

Modbus-specifikationen innehåller beskrivningar av hur felhantering ska skötas på protokollnivå, inklusive hur svarsmeddelanden ska se ut för olika typer av fel.

Informationssäkerhet

Modbus innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.10.5 Specifikationer

Modbus Application Protocol Specification V1.1b3. Modbus Organization. 2012.

Modbus Messaging on TCP/IP Implementation Guide V1.0b. Modbus Organization. 2006.

Modicon Modbus Protocol Reference Guide. PI–MBUS–300 Rev. J. 1996.

5.11 OPC

Open Platform Communications (OPC) är ett samlingsnamn för ett antal protokoll för kommunikation inom industriell automation. Protokollen är utformade för att överföra aktuell data, historisk data, larm/händelser och liknande över standardinfrastruktur som Ethernet och TCP/IP.

Den första versionen av OPC-specifikationen publicerades 1996 av en löst sammansatt grupp av företag som senare under samma år bildade OPC Foundation. När detta skrivs har OPC Foundation över 450 medlemsföretag[5].

OPC stod tidigare för *OLE for Process Control*, som visar på OPC-protokollens ursprung i funktionalitet i Microsofts operativsystem Windows. OLE, *Object Linking and Embedding*, är en Windows-specifik teknik för kommunikation mellan applikationer. OLE lanserades 1990 av Microsoft och tillät kommunikation mellan applikationer såväl inom en dator som mellan datorer.

Över tiden har OPC-protokollen frikopplats från OLE och stöd för protokollen finns nu under ett flertal operativsystem utöver Windows. Uttydningen av OPC ändrades år 2011 till det mer allmänna Open Platform Communications.

5.11.1 Varianter

OPC finns i två grundvarianter, den äldre OPC Classic och den nyare OPC Unified Architecture (UA).

OPC UA beskriver ett sammanhållet protokoll och definierar i dagsläget två underliggande bärare, antingen det egna protokollet UA TCP (över IP) eller standardprotokollet HTTPS (över TCP/IP). Tidigare fanns även standardprotokollet SOAP över HTTP med som bärare men denna har tagits bort till OPC UA version 1.03.

OPC Classic består av en samling av protokoll, alla definierade genom egna specifikationer, där dessa får anses utgöra kärnan:

- **OPC Data Access (DA)** – Protokoll för åtkomst till data mellan komponenter i ett styrsystem, exempelvis mellan SCADA-system och PLC.
- **OPC Historical Data Access (HDA)** – Protokoll för åtkomst till historiska data, typiskt använt mellan en klient (exempelvis en operatörsterminal) och en historik-server (eng. *historian*).
- **OPC Alarm and Events (A&E)** – Protokoll för att överföra larm och andra händelser mellan komponenter i ett styrsystem.

[5] https://opcfoundation.org/members [hämtat 2017-05-19].

Utöver dessa delar består OPC Classic av ytterligare fem delar som utökar funktionaliteten, bland annat genom stöd för autentisering i protokollen.

OPC UA bygger på OPC Classic och har samma grundfunktioner. OPC UA är strukturerad som ett ramverk där de applikationsnära protokollen sedan integreras. Detta speglas även i specifikationerna för OPC UA som består av totalt tretton delar där del 1–7 utgör en gemensam kärna (eng. *core*), del 8–11 beskriver applikationsnära funktioner och del 12–13 utgör stödfunktioner.

De applikationsnära funktionerna i OPC UA motsvarar de ovan listade varianterna i OPC Classic plus ett protokoll för att styra så kallade program (eng. *programs*), som är en typ av styrbara tillståndsmaskiner.

5.11.2 Användningsområde

Primär modellnivå	2. Produktionskontroll 3. Produktionsledning
OSI-lager	7. Applikationslager 6. Presentationslager 5. Sessionslager 4. Transportlager (UA TCP) (4. Transportlager [TCP])

5.11.3 Datamodell

OPC UA utgör en utökning av modellen i OPC Classic och är bakåtkompatibel med denna. Då likheterna är så pass stora mellan datamodellerna i OPC Classic och OPC UA så tar detta avsnitt endast upp datamodellen för OPC UA.

Datamodellen i OPC UA är komplex och baseras på objekt som består av såväl variabler som metoder. Variablerna i ett objekt kan innehålla data av många olika typer medan metoderna är funktioner som kan anropas av en kommunicerande part.

OPC UA definierar ett antal grundläggande datatyper, exempelvis numeriska värden, strängar, bilder, tidsstämplar och XML-data. Utöver detta går det även att definiera egna datatyper i form av objekttyper[6] som kan ses som en mall för andra objekt.

Objekten i en OPC UA-server ordnas enligt UPC UA:s informationsmodell. Denna modell bygger på en trädstruktur med en rotnod (eng. *root*) som innehåller grenar för vyer (eng. *views*), objekt (eng. *objects*) och typer (eng. *types*). Vyer och typer är speciella kategorier som definierar tolkningen av objekten.

[6] Objekttyper i OPC UA kan närmast liknas vid dynamiskt skapade klasser inom objektorienterad programmering. Objekttyper kan ses som mallar som används när objekt skapas.

Under objektgrenen finns ett serverobjekt samt ett godtyckligt antal undergrenar som innehåller alla dataobjekt i systemet. Serverobjektet definierar och beskriver servern och dess egenskaper.

5.11.4 Säkerhet

Driftsäkerhet

OPC förlitar sig på lägre protokollager för att hantera upptäckt av transmissionsfel, omsändningar och liknande. OPC UA beskriver i viss utsträckning hur kommunikationsfel ska hanteras i såväl protokollet som applikationen.

Informationssäkerhet

OPC Classic innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

Det finns en övergripande säkerhetsmålsättning beskriven i del 2 av specifikationerna för OPC UA, inklusive övergripande hot. Specifikationerna beskriver även en flexibel uppsättning skyddsåtgärder som kan implementeras i systemen om det ses som lämpligt. Specifikationerna sätter dock inga hårda krav på vilka skyddsåtgärder som implementeras i systemen.

De skyddsåtgärder som finns specificerade i OPC UA inkluderar autentisering av klienter och servrar, auktorisering (åtkomststyrning) av klienter, sekretesskydd och riktighetsskydd. OPC UA specificerar även mekanismer för att öka tillgängligheten under överbelastningsattacker samt åtgärder för spårbarhet genom exempelvis loggning av händelser.

5.11.5 Specifikationer

Data Access Custom Interface Standard Version 3.00. OPC Foundation 2003.

OPC Historical Data Access Specification Version 1.20. OPC Foundation 2003.

Alarms and Events Custom Interface Standard Version 1.10. OPC Foundation 2002.

OPC Unified Architecture Specification Part 1: Overview and Concepts. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 2: Security Model. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 3: Address Space Model. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 4: Services. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 5: Information Model. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 6: Mappings. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 7: Profiles. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 8: Data Access. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 9: Alarms and Conditions. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 10: Programs. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 11: Historical Access. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 12: Discovery. Release 1.03. OPC Foundation 2015.

OPC Unified Architecture Specification Part 13: Aggregates. Release 1.03. OPC Foundation 2015.

5.12 PROFIBUS

PROFIBUS, *Process Field Bus*, är en fältbuss som togs fram genom ett samarbete mellan ett antal företag och institut i Västtyskland under andra halvan av 1980-talet. PROFIBUS-protokollet skapades för att kunna använda decentraliserade (distribuerade) I/O-enheter till styrsystem, primärt för att spara kablage mellan en styrenhet och sensorer/aktorer i den fysiska processen. I början av 2000-talet togs PROFIBUS upp som ett av flera automationsprotokoll i standarderna IEC 61158 och IEC 61784.

Det grundläggande protokollet i PROFIBUS i nu gällande standarder är *PROFIBUS Decentralized Peripherals* (DP). PROFIBUS DP är ett master-slave-protokoll där kommunikationen går över seriella kanaler. Grunden i protokollet är en cyklisk pollning där en master frågar samtliga slavar som denne kommunicerar med på bussen. Utöver detta finns även acyclisk kommunikation, där en master kommunicerar med en slav vid behov.

I en situation med flera masters på en buss så regleras tillgången till bussen genom innehav av ett *token*, ett slags virtuell stafettpinne som överlämnas från master till master så att alla kan få tillgång till bussen.

Ovanpå PROFIBUS DP implementeras standardiserade så kallade applikationsprofiler (eng. *application profiles*), som beskriver gemensamma informationsmodeller för olika typer av utrustningar.

PROFIBUS DP kommunicerar via det underliggande protokollet *Fieldbus Data Link* (FDL) som överför paketorienterad data, där paketen kallas *telegram* i standarden. FDL transporteras i sin tur på ett fysiskt lager som kan utgöras av RS-485, MBP (Manchester coded, bus power) eller optisk media. MBP är ett fysiskt lager där spänningsmatning av slaven kan ske genom samma kablar som överför protokollet, vilket kan spara kabeldragning genom att yttre spänningsmatning inte behövs.

Inom samarbetet som ursprungligen specificerade PROFIBUS togs det fram flera fältbussprotokoll avsedda för olika användningsområden. Protokollen har vissa gemensamma egenskaper som gör att integration och översättningar mellan protokoll är möjlig i vissa fall, något som exemplifieras av applikationsprofilen för att kapsla in HART-fältbussprotokollet över PROFIBUS DP.

5.12.1 Varianter

PROFIBUS finns i två varianter i standarden:

- **PROFIBUS Decentralized Peripherals (DP)** – Fältbussprotokoll för att kommunicera mellan ett styrsystem, exempelvis en PLC, och distribuerade sensorer, aktorer och I/O-enheter.

- **PROFIBUS Process Automation (PA)** – Fältbussprotokoll med samma kommunikationsprotokoll som PROFIBUS DP men med begränsningar på det fysiska lagret för att fungera i explosiva eller brandfarliga miljöer. PROFIBUS PA kan närmast liknas vid en sorts applikationsprofil för PROFIBUS DP men är explicit specificerad i standarden till skillnad från andra applikationsprofiler.

Den ursprungliga varianten **PROFIBUS Fieldbus Message Specification (FMS)** används normalt sett inte längre och finns inte med dagens standarder.

När detta skrivs finns det ett tjugotal applikationsprofiler för PROFIBUS. Specifikationerna för applikationsprofilerna ingår inte i standarden utan tillhandahålls av PI Organization till dess medlemmar[7].

5.12.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 6. Presentationslager (2. Datalänklager) (1. Fysiskt lager)

5.12.3 Datamodell

PROFIBUS bygger på en objektorienterad datamodell där olika funktioner i enheterna grupperas i applikationsprocessobjekt (APO). APO:er innehåller funktioner i form av tjänster (eng. *services*) och information i form av attribut (eng. *attributes*). Attributen kan vara av olika typer, såväl standarddatatyper som egendefinierade datatyper.

Applikationsprofilerna definierar vilka specifika objekt en enhet ska implementera utöver de generella objekt som alltid ska finnas i PROFIBUS-enheter.

5.12.4 Säkerhet

Driftsäkerhet

Överföringsfel på PROFIBUS-telegram upptäcks genom en checksumma i varje telegram. PROFIBUS-standarden specificerar en mängd funktioner för felhantering, inklusive funktioner för diagnostik av överföringsproblem.

[7] http://www.profibus.com/download/profiles/ [hämtat 2017-05-19]

Informationssäkerhet

PROFIBUS innehåller inga specifika säkerhetsmekanismer för informationssäkerhet.

5.12.5 Specifikationer

Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series. IEC 61158-1:2014.

Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition. IEC 61158-2:2014.

Industrial communication networks – Fieldbus specifications – Part 3-3: Data-link layer service definition – Type 3 elements. IEC 61158-3-3:2014.

Industrial communication networks – Fieldbus specifications – Part 4-3: Data-link layer protocol specificationn – Type 3 elements. IEC 61158-4-3:2014.

Industrial communication networks – Fieldbus specifications – Part 5-3: Application layer service definition – Type 3 elements. IEC 61158-5-3:2014.

Industrial communication networks – Fieldbus specifications – Part 6-3: Application layer protocol specification – Type 3 elements. IEC 61158-6-3:2014.

Industrial communication networks – Profiles – Part 1: Fieldbus profiles. IEC 61784-1:2014.

Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3. IEC 61784-3-3:2016.

Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3. IEC 61784-5-3:2013.

5.13 PROFINET

PROFINET, *Process Field Net*, är ett automationsprotokoll för kommunikation över Ethernet i industriella miljöer. PROFINET är, trots likheten i namnet, inte en direkt vidareutveckling av PROFIBUS utan bygger endast delvis på samma grund och samma standarder.

PROFINET använder Ethernet för det fysiska lagret och datalänklagret. TCP/IP används för kommunikation som inte är tidskritisk, medan tidskritisk information överförs via de egna protokollen *Real-Time* (RT) och *Isochronous Real-Time* (IRT). Med protokollet IRT kan uppdateringsintervallet under specifika förutsättningar nå ner till 31,25 µs.

PROFINET har samma grundläggande struktur som PROFIBUS, med ett master-slave-förhållande och erbjuder såväl cyklisk som acyklisk kommunikation mellan dessa. Den cykliska kommunikationen använder RT- och IRT-protokollen medan den acykliska kommunikationen går över TCP/IP.

5.13.1 Varianter

PROFINET har bara en protokollvariant, PROFINET IO, som har delats upp i funktionsgrupper som bygger på varandra, så kallade *conformance classes* (CC). En PROFINET-enhet behöver inte implementera alla CC-nivåer.

CC-nivåerna är följande:

- **PROFINET IO CC-A** – Grundläggande funktioner för realtidskommunikation. Enheten ska implementera protokollen TCP/IP och RT.
- **PROFINET IO CC-B** – Utökning av CC-A med diagnostiska funktioner.
- **PROFINET IO CC-C** – Utökning av CC-B med hårdvarustöd för bandbreddsreservation på Ethernet-länken. Enheten ska även implementera protokollet IRT.

5.13.2 Användningsområde

Primär modellnivå	1. Direktkontroll 2. Produktionskontroll
OSI-lager	7. Applikationslager 4. Transportlager (RT/IRT) 3. Nätverkslager (RT/IRT)

5.13.3 Datamodell

PROFINET bygger på en datamodell med liknande egenskaper som för PROFIBUS. Samma applikationsprofiler används för båda protokollen.

5.13.4 Säkerhet

Driftsäkerhet

PROFINET har grundläggande funktioner för felupptäckt och återsändningar när så är lämpligt. Det finns stöd för att skicka personsäkerhetsrelaterad information med protokollet, bland annat genom applikationsprofilen PROFIsafe.

Informationssäkerhet

PROFINET innehåller inga specifika säkerhetsmekanismer för informations-säkerhet.

5.13.5 Specifikationer

Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series. IEC 61158-1:2014.

Industrial communication networks – Fieldbus specifications – Part 5-10: Application layer service definition – Type 10 elements. IEC 61158-5-10:2014.

Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements. IEC 61158-6-10:2014.

Industrial communication networks – Profiles – Part 1: Fieldbus profiles. IEC 61784-1:2014.

Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3. IEC 61784-3-3:2016.

Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3. IEC 61784-5-3:2013.

6 Ordlista

Tabell 4. Ordlista.

Term	Förklaring
DUC	Datorundercentral, en typ av programmerbart styrsystem.
Halv duplex	Kommunikation kan ske i båda riktningarna men endast en riktning i taget.
ICS	Industriella informations- och styrsystem (eng. *industrial control system*)
Master	Den part i ett master-slave-protokoll som initierar kommunikationen.
Multidrop	Flerpunktskommunikation där flera anslutna enheter kan kommunicera över ett gemensamt, delat medium.
PLC	Programmerbart styrsystem (eng. *programmable logic controller)*.
RS-232	En standard för elektrisk kommunikation mellan datorer och kommunikationsutrustning. RS-232 kopplas direkt mellan två enheter och tillåter avstånd upp till c:a 15 m.
RS-422	En standard för differentiell elektrisk kommunikation över tvinnade par. RS-422 är enkelriktad men kan ha flera lyssnande enheter inkopplade. RS-422 tillåter avstånd upp till c:a 1500 m vid låg hastighet.
RS-485	En standard för differentiell elektrisk kommunikation över tvinnade par. RS-485 tillåter multidrop-kommunikation i halv duplex. RS-485 tillåter avstånd upp till c:a 1200 m vid låg hastighet.
RTU	Remote terminal unit, en typ av programmerbart styrsystem.
SCADA	Supervisory control and data acquisition.
Slav	Eng. *slave*, den part i ett master-slav-protokoll som väntar på ett meddelande från en master innan den svarar. Slaven är typiskt passiv så länge den inte har blivit anropad av mastern.

Strömslinga	Eng. *current loop*, teknik för elektrisk kommunikation mellan två enheter där signaleringen görs genom elektrisk ström (snarare än elektrisk spänning).

Referenser

IEEE (1985). *IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.* IEEE 802.3-1985.

IEEE (1998). *Logical Link Control,* IEEE 802.2-1998.

IEC (2013*). IEC 62264-1:2013 Enterprise-control system integration*. (IEC 62264-1:2013). International Electrotechnical Commission. enève: IEC.

IETF (1989). *RFC 1122 Requirements for Internet Hosts -- Communication Layers.* https://tools.ietf.org/html/rfc1122 (läst 2016-11-13).

ISA (2010). ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration - Part 1: Models and Terminology. International Society of Automation.

ISO/IEC (1989) Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, ISO 7498-2:1989.

ISO/IEC (1994). ISO/IEC 7498-1 Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994(E).

ISO/IEC (2015). ISO/IEC 8824-1:2015. Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation.

Williams, T.J. (red.) (1989). *A Reference Model for Computer Integrated Manufacturing.* Research Science Park: Instrument Society of America.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se