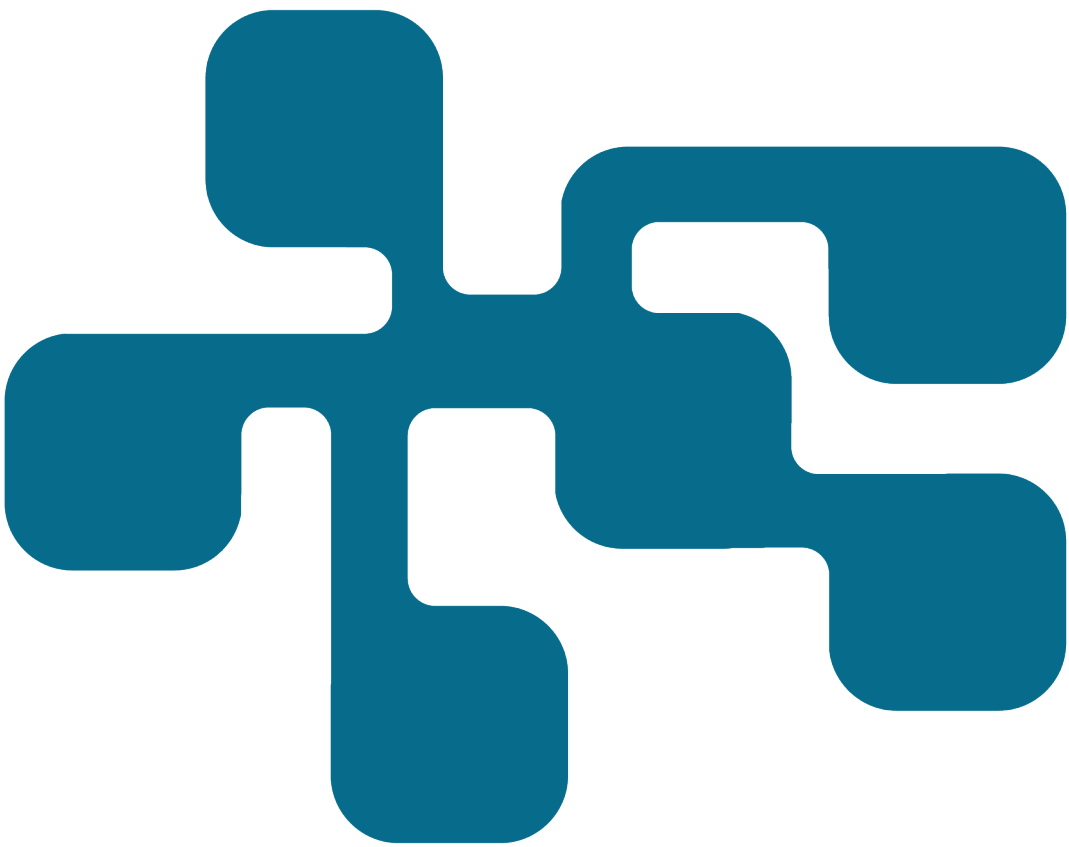
Teoretisk referensmiljö för industriella informations- och styrsystem

LARS WESTERDAHL, CHRISTIAN VALASSI,
DANIEL EIDENSKOG, PETER ANDERSSON, ERIK WESTRING



FOI-R--4633--SE
ISSN 1650-1942 Maj 2020

Lars Westerdahl, Christian Valassi, Daniel Eidenskog, Peter Andersson, Erik Westring

Teoretisk referensmiljö för industriella informations- och styrsystem

Titel	Teoretisk referensmiljö för industriella informations- och styrsystem
Title	Theoretical reference model for industrial control systems
Rapportnr/Report no	FOI-R--4633--SE
Månad/Month	Maj/May
Utgivningsår/Year	2020
Antal sidor/Pages	49
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E324554
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Det kan vara komplext att diskutera säkerhetsproblem och säkerhetslösningar för industriella informations- och styrsystem utifrån en modell. Om modellen har för hög abstraktionsnivå kan det vara svårt att konkretisera relaterade problem och lösningar. Samtidigt kan det vara olämpligt att modellera existerande system i alltför hög detaljgrad eftersom dessa typer av system ofta skiljer sig mellan installationer, vilket innebär att modellen då inte blir tillräckligt generell. Dessutom riskerar en detaljerad modell att innehålla känslig information som kan utnyttjas av tredje part. För att lösa detta problem krävs en modell som är tillräckligt detaljrik för att möjliggöra diskussioner kring säkerhetsproblem och säkerhetslösningar. Samtidigt behöver modellen vara på en tillräckligt generell nivå för att kunna beskriva industriella informations- och styrsystem för ett stort antal olika branscher som nyttjar denna typ av system.

Denna rapport beskriver en teoretisk referensmiljö i form av en modell med målet att denna öppet kan användas för att diskutera hot, sårbarheter och säkerhetsåtgärder för industriella informations- och styrsystem. Syftet med rapporten är att öka förståelsen för dessa system och förenkla kunskapsspridningen inom området utan att äventyra informationssäkerheten för en specifik installation. Rapporten beskriver utöver modellen även olika typer av industriella informations- och styrsystem, processer och tillämpningar samt exponeringsytor och exempel på tidigare angrepp. Modellen demonstreras även i form av två typfallsexempel i syfte att ge läsaren en förståelse för hur modellen kan användas i praktiken.

Nyckelord: Industriella informations- och styrsystem

Summary

It can be a complex issue to discuss security problems and security solutions for industrial information and control systems based on a model. If the model has a high level of abstraction, it will be difficult to concretize related problems and solutions. At the same time, it may be inappropriate to model existing systems in too high a degree of detail since these types of systems often differ between installations, which means that the model will then not be sufficiently generalizable. In addition, a detailed model risks containing sensitive information that can be used by third parties. To solve this problem, a model that is sufficiently detailed to enable discussions about security problems and security solutions is required. At the same time, the model needs to be at a sufficiently general level to be able to describe industrial information and control systems for a large number of different industries that use these types of systems.

This report describes a theoretical reference environment in the form of a model with the goal that it can be used publicly to discuss threats, vulnerabilities and security measures for industrial information and control systems. The purpose of the report is to increase the understanding of these systems and to simplify the dissemination of knowledge in the area without compromising information security for a specific installation. In addition to the model, the report also describes different types of industrial information and control systems, processes and applications as well as exposure areas and examples of previous attacks. The model is also demonstrated in the form of two case examples with the purpose of providing the reader with an understanding of how the model can be used in practice.

Keywords: Industrial Control Systems

Innehållsförteckning

1 Inledning

I denna rapport presenteras en teoretisk referensmiljö för industriella informations- och styrsystem. Referensmiljön är en generalisering av flera olika verksamhetsområden, vilket innebär att referensmiljön inte i detalj avbildar en existerande miljö. Denna teoretiska referensmiljö täcker bland annat informationsflöden och teknik på flera nivåer, från affärsledning till fysisk process.

Framtagning av en teoretisk referensmiljö har utförts på uppdrag av *Myndigheten för samhällsskydd och beredskap* (MSB) inom ramen för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3).

1.1 Problemställning

Det kan vara problematiskt att diskutera och konkretisera säkerhetsproblem eller säkerhetslösningar relaterat till industriella informations- och styrsystem. Ett sätt att förenkla detta är att använda avbildningar eller modeller av industriella informations- och styrsystem. Avbildningarna kan i detta fall bidra till en ökad förståelse hos de individer som deltar diskussionen.

Avbildningar och modeller kan dock i sig vara problematiska att använda. Om abstraktionsnivån är för hög kan det vara svårt att hitta och konkretisera säkerhetsproblem och säkerhetslösningar på detaljnivå. Om abstraktionsnivån istället är för låg riskerar avbildningen eller modellen att bli för specifik och därmed icke-generaliserbar. Detta eftersom industriella informations- och styrsystem på detaljnivå ofta skiljer sig mellan installationer. Således blir avbildningen endast relevant för ett fåtal specifika installationer.

Avbildningar av existerande system och nätverk är ofta en god idé för internt bruk men kan vara problematiska om avbildningen ska användas externt eller i ett publikt forum. Detta eftersom informationen i avbildningen riskerar att utsätta systemet och dess ägare för ett onödigt risktagande då systemet och dess arkitektur kan exponeras för tredje part.

För att öppet kunna diskutera säkerhetsproblem och säkerhetslösningar för industriella informations- och styrsystem utanför organisationsgränser krävs det därför modeller av en mer generell natur. Det är dock viktigt att dessa modeller inte skapas på en så hög abstraktionsnivå att viktiga sårbarheter riskerar att utelämnas.

1.2 Mål och syfte

Studiens mål är att identifiera en teoretisk referensmiljö som kan användas för att resonera kring risker, hot och sårbarheter avseende industriella informations- och styrsystem. Detta för att öka förståelsen för dessa system och förenkla kunskapsspridningen inom området utan att äventyra informationssäkerheten för specifika system.

1.3 Avgränsning

Industriella informations- och styrsystem används i otaliga tillämpningar. En referensmiljö som i detalj är heltäckande för alla olika tillämpningsområden skulle därför bli allt för komplex. Av denna anledning är den identifierade modellen beskriven på en mer generell nivå, men med goda förutsättningar att kunna kompletteras med detaljer som reflekterar ett specifikt tillämpningsområde eller system.

1.4 Genomförande

Inledningsvis genomfördes en litteraturstudie i syfte att identifiera relevanta generella modeller samt bakgrundsinformation gällande vanliga arkitekturer för industriella informations- och styrsystem. Därefter analyserades de valda modellerna utifrån den beskrivning som ges i kapitel 5. En fördjupande litteraturgenomgång genomfördes sedan i syfte att anskaffa kunskap angående arkitekturerna för de valda typfallsexemplen, därefter utvecklades den valda modellen och applicerades på de båda typfallen.

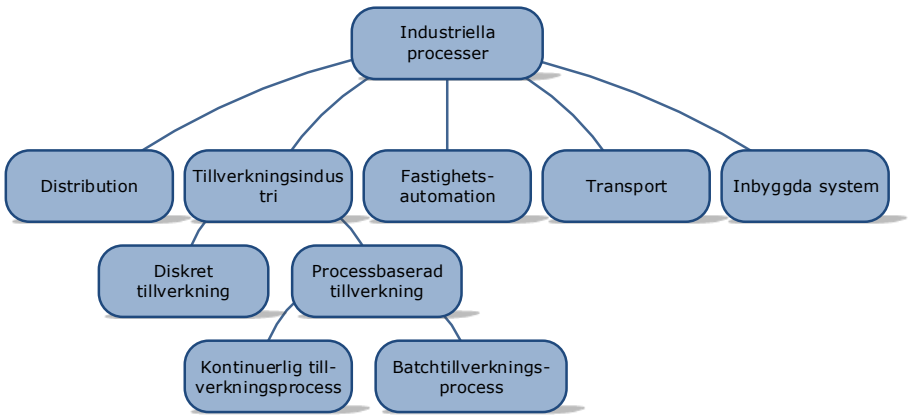
1.5 Rapportens struktur

Rapporten är indelad i sju kapitel. De första fyra kapitlen syftar till att belysa olika delar av bakgrundsarbetet. Kapitel 1 introducerar rapporten, dess mål och avgränsningar. Kapitel 2 beskriver de olika processerna som existerar inom ett industriellt system. Kapitel 3 beskriver dessa system mer detaljerat. Kapitel 4 introducerar vedertagna modeller för att beskriva industriella informations- och styrsystem.

Rapporten går sedan vidare med kapitel 5 som beskriver den modellanalys som gjorts och bakomliggande resonemang kring valet av modell. Kapitel 6 presenterar den valda modellen och applicerar denna på två typfallsexempel. Avslutningsvis diskuterar kapitel 7 den framtagna modellen och dess relevans, syfte samt applikationsområde.

2 Processer

Modeller av industriella processer beskriver oftast på vilket sätt ett resultat tas fram, men kan även beskriva vilken miljö som resultatet tillämpas inom. Vad resultatet är varierar beroende på vad syftet med systemet är. Ordet *industriella* ger lätt en bild av fabriksmiljöer, vilket är en viktig del av industriella processer genom diskret och processorienterad tillverkning. I industriella processer ingår dock även distributionssystem för exempelvis el och vatten samt andra varianter av distributionssystem, såsom transportsystem för tåg och flyg, men även fastighetsautomation och inbyggda system (Figur 1) (Stouffer, Pillitteri, Lightman, Abrams & Hahn 2015; Galloway & Hancke 2013). Industriella processer har således tillämpningar som inte alltid är så industriella.



Figur 1. Industriella processer baserat på NIST (Stouffer et al. 2015) samt Galloway och Hancke (2013).

2.1 Tillverkningssystem

Industriella processer för tillverkningssystem delas in i *diskret tillverkning* och *processbaserad tillverkning*. Den processbaserade tillverkningen delas vidare in i *kontinuerlig tillverkningsprocess* och *batchtillverkningsprocess.*

2.1.1 Diskret tillverkning

Vid en diskret tillverkningsprocess sätts en produkt samman av olika delar enligt en produktstruktur[1]. Alla ingående delar och den resulterande produkten befinner sig hela tiden i ett stabilt tillstånd. Det innebär att produktionen kan delas upp i steg och att eventuella fördröjningar inte skadar produkten. Ofta sker diskret produktion i celler där specifika och bitvis komplexa moment utförs, för att sedan skicka produkten vidare till nästa cell. Diskret produktion är exempelvis vanlig inom fordonsindustrin och elektronikindustrin.

2.1.2 Processbaserad tillverkning

Under processbaserad tillverkning skapas en produkt genom en process som inte kan, eller inte bör brytas eftersom ett avbrott kan medföra risk för allvarliga skador på människor eller utrustning och i värsta fall leda till att människoliv går förlorade. Det ingående materialet som krävs för slutprodukten blandas eller transformeras enligt ett recept och den resulterande slutprodukten är något som inte utan ansträngning kan reverseras. Processbaserad tillverkning är antingen en kontinuerlig tillverkningsprocess eller en batchtillverkningsprocess.

Kontinuerlig process

Vid en kontinuerlig process skapas en produkt så länge som ingående delar fylls på. Exempel på kontinuerliga processer är energiproduktion och raffinaderier. Under energiproduktion omvandlas exempelvis vattens rörelseenergi via en turbin till elektricitet. Så länge vattnet fortsätter att strömma genom turbinen fortsätter elektriciteten att genereras. Det samma gäller för ett raffinaderi, där diesel och bensin utvinns ur råolja. Så länge råolja tillförs pågår processen och mer bränsle utvinns.

Batchtillverkning

I en batchtillverkningsprocess delas processen upp i steg där varje steg har en egen process som körs från början till slut. Mellan varje steg har produkten ett stabilt tillstånd, men under ett utvecklingssteg får inte processen avbrytas. En batch utgör en bestämd mängd råvaror som förbrukas under tillverkningssteget och resultatet kan beskrivas som kommande från en specifik batch. Även om en batchtillverkningsprocess kan delas upp i steg, är den inte diskret. Under processens gång har de ingående råvarorna förändrats och kan inte återföras till sitt ursprungliga tillstånd. Batchtillverkning är vanligt inom exempelvis livsmedels- och läkemedelsindustrin.

[1] Eng. *Bill of Material* (BOM).

2.2 Distributionssystem

Distributionssystem används för att frakta en produkt från produktionsplatsen till en konsument. Typiskt för distributionssystem är stora avstånd mellan producent och konsument, men även att produkten inte kan paketeras på något praktiskt sätt. Produkten i dessa fall kan exempelvis vara elektricitet, naturgas, dricksvatten eller avloppsvatten.

I de flesta fall kan distributionssystem delas in i tre områden: *produktion*, *transmission* och *distribution*. Produktionsplatserna är ofta belägna långt ifrån konsumenterna, vilket gör att stora mängder av produkten behöver flyttas långa sträckor. Förflyttningen sker genom transmissionssystem vilka kan hantera stora flöden över långa avstånd. Närmast konsumenten finns distributionssystemen vilka ansluter till konsumentens fastighet eller en försäljningsplats, exempelvis en tankstation för naturgas.

2.3 Transportsystem

Transportsystem kan vara svåra att se som industriella informations- och styrsystem, då industriella informations- och styrsystem ofta förknippas med någon form av produktion. Ett transportsystem kan dock ha stora likheter med ett distributionssystem i sin tillämpning. Tåg- och flygtrafik är exempel på system som täcker stora geografiska ytor, som är säkerhetskritiska och som har ett stort behov av övervakning. Eftersom dessa system involverar människor direkt i processen, till skillnad från varuproduktion, ökar även kraven på säkerhet drastiskt då konsekvenserna av olyckor är mycket stora.

2.4 Fastighetsautomationssystem

För moderna fastigheter finns det behov av att övervaka miljön i fastigheten med målsättningen att minska energiåtgången. Syftet med detta är att minimera miljöpåverkan samt att minska kostnaderna. Alla fastigheter utgör inte kritisk infrastruktur men för vissa verksamheter, exempelvis sjukvård, finns särskilda krav och en annan målsättning. Inom sjukvården ställs bland annat krav på reservkraft och specifik inomhustemperatur för att kunna genomföra operationer.

2.5 Inbyggda system

Industriella processer återfinns även i mindre system såsom fordon. Moderna fordon använder exempelvis industriella informations- och system eller i alla fall cyberfysiska system via kommunikationsbussen, för att bland annat optimera motorn till att vara så miljövänlig som möjligt. Många andra funktioner, såsom

antisladdsystem, bromsar och styrning kontrolleras även av datorer som kommunicerar över kommunikationsbussen.

Flera interna fordonssystem kan även nås på distans och används bland annat av tillverkare för diagnostik och vägassistans. Fjärranslutningsmöjligheter kan dock också innebära en sårbarhet eftersom interna fordonssystem ofta har bristande säkerhet (Thuen 2016).

3 Industriella informations- och styrsystem

Industriella processer måste hanteras av människor och teknik. Dagens industriella informations- och styrsystem har utvecklats från att vara reglersystem med en dedikerad kommunikationskanal via telenätet till att vara datorsystem med möjlighet att kommunicera över internet.

Begreppet industriella informations- och styrsystem omfattar de datorsystem som lagrar och bearbetar information i en automationsmiljö samt de datorsystem som övervakar den fysiska processen. Dessa system är oftast även sammankopplade med administrativa system i en kontorsmiljö samt mot supportleverantörer. Då industriella informations- och styrsystem i ena änden är kopplade till en fysisk process ställs höga krav på korrekthet och tillgänglighet, ofta med realtidskrav. Efter hand som information rör sig från den fysiska processen till de administrativa systemen minskar exempelvis kraven på realtid till förmån för kontorsmässig databehandling.

Det finns flera begrepp med mer eller mindre samma innebörd som industriella informations- och styrsystem. Dels används svenska begrepp såsom industriella kontrollsystem eller styrsystem, dels används engelska begrepp såsom *Industrial Control Systems* (ICS).

Industriella informations- och styrsystem kan kategoriseras i olika typer beroende på vilken process de ska hantera (Stouffer et al. 2015). I avsnitten som följer presenteras tre typer: *SCADA-system*, *distribuerade kontrollsystem*, och *fristående styrsystem*. Dessa tre typer representerar majoriteten av alla varianter för industriella informations- och styrsystem. De ingående komponenterna i dessa tre presenterade typer av system presenteras sedan i kapitlets avslutande avsnitt.

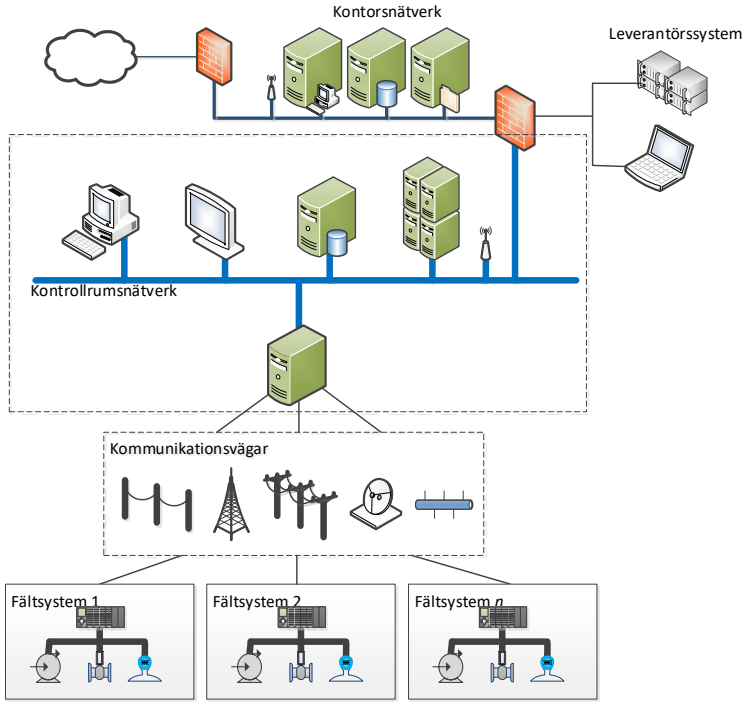
3.1 SCADA-system

Supervisory Control and Data Acquisition (SCADA) är en typ av industriella informations- och styrsystem som används för övervakning av processer. Traditionella användningsområden för SCADA-system är övervakning av processer som är utspridda över ett stort geografiskt område, exempelvis övervakning av transmission och distribution av elkraft.

Stora avstånd medför att SCADA-system måste kunna hantera fel som uppkommer på grund av fördröjningar och bortfall i kommunikationen, vilka försvårar en kontinuerlig kommunikation. Detta medför att det blir svårt för en operatör att direkt påverka en process. Centralt för ett SCADA-system blir

således datainsamling och presentation av data för övervakningen av processer. Processnära delsystem kontaktar den centrala övervakningsservern vid behov, exempelvis vid larm. Operatörens uppgift blir att sätta gränsvärden och reagera på larm från delsystem. Detta fokus på datainsamling sätter kontrollrummet, och kanske främst SCADA-servern, i centrum. Delprocesserna behöver ofta kunna agera med en hög grad av autonomitet eftersom dessa processer tenderar att vara utspridda geografiskt samt att kommunikationen mellan delprocess och SCADA-server är begränsad i överföringshastighet.

Centralt för ett SCADA-system är *SCADA-servern*, ibland även kallad *Master Terminal Unit* eller *Master Telemetry Unit*. Det är med SCADA-servern som delprocesser kommunicerar och det är via SCADA-servern som operatören kommunicerar ut gränsvärden för delprocesserna (Figur 2). De larm och värden som skickas till SCADA-servern sparas i en *Historian* – en databas med hög prestanda. Operatören övervakar processen via ett *Human-Machine-Interface* (HMI). Genom HMI kan operatören kvittera de larm som inkommer samt ändra gränsvärden för dessa larm. SCADA-servern och Historian har ett begränsat stöd för att genomföra analyser. För mer utförliga analyser och presentation av trender används därför särskilda program vilka är åtkomliga från *applikationsservrar*. I de underliggande anläggningarna där delprocesser utförs finns fältsystemen. För fältsystemen är en styrdator, ofta kallad RTU från engelskans *Remote Terminal Unit*, central genom att den samlar in information från sensorer och värderar denna med hjälp av ett program. RTU:n skickar periodiserade uppdateringar till SCADA-servern samt larm om ett värde går utanför ett satt gränsvärde.



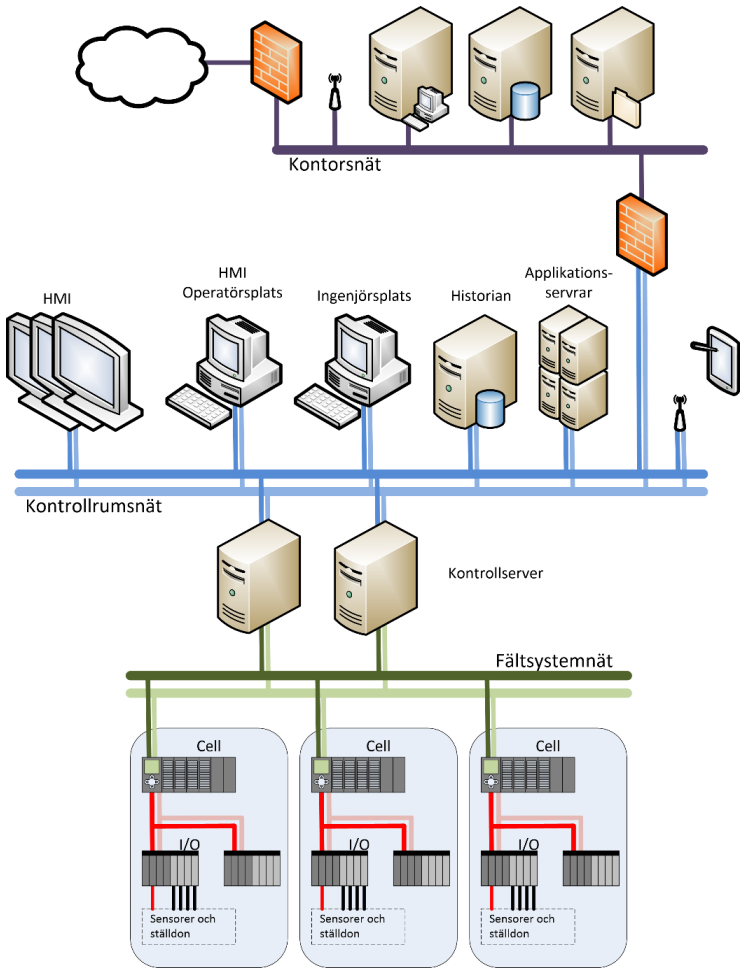
Figur 2. Översiktsbild av ett SCADA-system.

3.2 Distribuerade kontrollsystem

Distribuerade kontrollsystem, från engelskans *Distributed Control System* (DCS), tillämpas huvudsakligen inom tillverkningsindustrin, och då främst för kontinuerliga processer eller batchprocesser. En kontinuerlig process är typiskt en process som är pågående över tid, vilket gör den känslig för störningar. Exempel på en sådan process är energiproduktion. Batchprocesser är vanliga inom exempelvis livsmedelsindustrin, men kan även vara ett delmoment inom exempelvis ett raffinaderi. Figur 3 visar en översiktlig exempelarkitektur för ett DCS.

Ett DCS är ett system som är designat för att kontrollera en komplex process. I ett DCS rör sig en produkt genom flera förädlings- eller omvandlingssteg till ett slutgiltigt tillstånd. En operatör kan inte nödvändigtvis kontrollera varje delmoment utan ser till att produktionen flyter mellan respektive moment. Operatören följer processen ifrån ett kontrollrum. Till skillnad från SCADA-system är det istället HMI:t som står i centrum för ett DCS, vilket innebär att det är viktigt att operatören kan följa processen eftersom denne ges ett större utrymme för kontroll av processen än för SCADA-system (Figur 3).

Hastighet och tillförlitlighet är viktigt i ett DCS. I och med att det är ett lokalt system används därför överlag lokala nätverk med IP-baserad trafik. Närheten och kapaciteten i nätverket medför att kontrollrummet regelbundet kan hämta information från styrdatorer när så önskas samt styra händelser i produktionen. Detta innebär att ett DCS ges större möjlighet för kontroll och styrning än ett SCADA-system

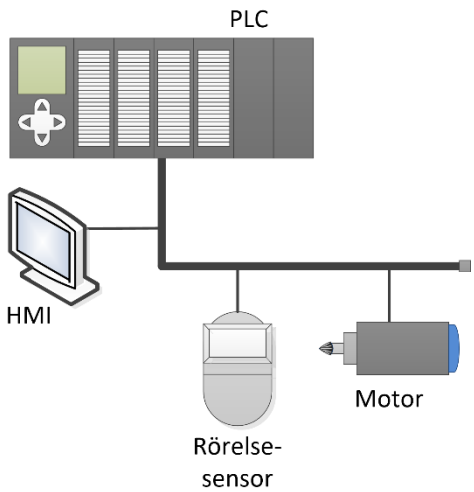


Figur 3. Exempelarkitektur för ett distribuerat kontrollsystem.

3.3 Fristående styrsystem

Alla industriella informations- och styrsystem är inte övervakade eller direkt påverkade från ett kontrollrum. Inbyggda system eller tydligt avgränsade och kontinuerliga uppgifter i ett större system kan fungera självständigt utan central

övervakning. En *Programmable Logic Controller* (PLC) är den centrala komponenten i ett sådant system, vilken har sina specifika uppgifter inprogrammerade i sitt minne. Systemets process kan ses genom ett HMI, men det är inte alltid säkert att denna typ av system har ett grafiskt gränssnitt. En generisk bild av ett fristående styrsystem visas i Figur 4.



Figur 4. PLC-baserat system.

3.4 Komponenter

Industriella informations- och styrsystem är i stort sett uppbyggda av likadana eller liknande komponenter oavsett syfte. Viss skillnad kan finnas exempelvis mellan SCADA-system och DCS, men skillnaden handlar mer om namngivningskultur än skillnader i förmåga. I detta avsnitt presenteras de vanligaste komponenterna som återfinns i industriella informations- och styrsystem.

3.4.1 Sensorer, motorer och ställdon

Det industriella informations- och styrsystemet får information om aktuell status i de olika processtegen via sensorer. Sensorinformationen kan vara binär eller analog. Ett binärt värde kan exempelvis vara ett gränsvärde där gränsen utgör det binära tillståndet, medan ett analogt värde uttrycker ett mätvärde såsom en temperatur. Kontrollsystem påverkar även processer genom ställdon och motorer exempelvis i syfte att öppna eller stänga ventiler och pumpar.

3.4.2 Insamling och styrning

Den information som sensorer samlar in går till en styrdator som även ger kommandon till ställdon och motorer. Det finns ett flertal olika styrdatorer med olika egenskaper, beroende på när de tagits fram och i vilken miljö de ska fungera inom. Gemensamt för alla styrdatorer är dock att de är skapade för att vara i en fysiskt krävande miljö.

PLC

En *Programmable Logic Controller* (PLC) kan ha flera uppgifter. Dels är en PLC en dator som fångar upp sensordata och vidarebefordrar dessa till en Historian, dels är det en dator som tar emot instruktioner och skickar dessa vidare till ställdon och motorer. En PLC har också möjlighet att på egen hand helt hantera en del av en process, exempelvis genom att reagera på sensordata enligt ett förbestämt mönster.

RTU

Remote Terminal Unit även kallad *Remote Telemetry Unit* (RTU) är en föregångare till PLC och används inom SCADA-system. I SCADA-system är det primärt övervakning av processer som genomförs, vilket medför att en RTU behöver kunna fånga upp och förmedla sensordata samt vidarebefordra kommandon till ställdon. Vid behov av ytterligare logik hanteras detta utanför RTU:n. I dagsläget ersätts bitvis RTU:er med PLC:er då dessa är billigare.

PAC

Programmable Automation Controller (PAC) är en nyare form av styrdator vilken sammanför funktionaliteten från en PLC med kapaciteten av en PC. En PAC blir således en mångsidig produkt anpassad för en nätverksmiljö.

IED

Intelligent Electronic Device (IED) är en kombination av styrdator och sensorer som främst används inom energisystem. En IED kan styra lokala händelseförlopp genom att läsa av sensordata och justera den lokala processen därefter, samt kommunicera resultat direkt med SCADA-servern.

3.4.3 Övervakning

Övervakning är en central del i alla typer av industriella informations- och styrsystem, för att försäkra sig om att alla delar av processen och dess komponenter uppträder på ett korrekt sätt. Nedan följer de komponenter i ett industriellt information- och styrsystem som är specifikt kopplade till övervakning.

Applikationsserver

En applikationsserver innehåller de program som används för att analysera data som samlats in från PLC:er eller RTU:er och som lagras i en Historian.

Operatörsstation

Operatören kan vid en operatörsstation (eng. *engineering workstation*) påverka ett DCS genom att exempelvis ändra kontrollvärden eller skapa nya kontrolloopar. En operatörsstation utgörs vanligtvis av en persondator med särskild programvara.

Historian

En Historian är en databas med hög kapacitet att ta emot uppdateringar. Alla sensordata som samlas in via PLC:er och RTU:er, samt de styrordrar och styrkommandon som skickas till ställdon lagras i Historian.

HMI

Ett HMI är en grafisk översikt av den process som övervakas och det medger även operatören att sända styrkommandon. Det finns flera olika typer av HMI, dels stora HMI där en överblick presenteras via en arbetsstation eller som en större panel, dels små HMI anslutna direkt till exempelvis en ventil eller undercentral.

SCADA-server

SCADA-servern, även kallad *Master Terminal Unit* (MTU), är central inom ett SCADA-system. Servern kommunicerar med RTU:er eller PLC:er för att samla in mätvärden eller ändra kontrollvärden. Insamlade data lagras i en Historian och presenteras i ett HMI.

Processkontrollenhet

Varje delsystem eller cell i ett DCS kontrolleras av en kontrollenhet. I denna enhet samlas sensordata in och omvandlas av kontrollenheten till styrkommandon enligt en förprogrammerad logik.

4 Generiska modeller

Det finns flera sätt att beskriva industriella informations- och styrsystem då dessa är komplexa system med många olika användningsområden. I detta kapitel beskrivs system utifrån ett organisatoriskt- och ledningsnivåperspektiv samt ett dataflödesperspektiv. Dessa perspektiv indikerar vad som står i fokus för modellen i fråga.

4.1 Övergripande modeller

De modeller som beskrivs nedan är allmänt vedertagna och används för att beskriva industriella informations- och styrsystem ur olika perspektiv.

4.1.1 Automationspyramiden

Automationspyramiden beskriver industriella informations- och styrsystem ur ett hierarkiskt perspektiv.

Figur 5. Automationspyramiden.

De nedre nivåerna är de som har direktkontakt med den process som stöds. På *fältnivån* finns utrustning för att mäta och påverka den process som hanteras. Mätningarna kan vara analoga för att ange rörliga värden, eller binära för att kontrollera om en sensor eller motor är aktiv eller inte. *Kontrollnivån* tolkar mätdata och styr delprocessen genom att påverka motorer och ställdon. Det är på dessa två nivåer som typiska automationsuppgifter utförs. Från kontrollnivån samlas även data in för vidarebefordran till *övervakningsnivån*. Övervakning av processer sker ofta på en annan plats än där mätning och styrning sker. Detta medför att övervakningsnivån måste fånga upp sensordata och uttrycka denna på

ett förståeligt sätt för de operatörer som arbetar i kontrollrummet. Processen underhålls via *planeringsnivån*. För att kunna fatta konkreta beslut som påverkar processen behövs information från produktionen, men planeringsbesluten realiseras inom övervakningsnivån. På den högsta nivån, *ledningsnivån*, hanteras affärsmässiga beslut, exempelvis försäljning av produktion och mottagande av beställningar.

4.1.2 ISA-95

ISA-95 är en standard från *International Society of Automation* (ISA)[2] vilken syftar till att definiera gränsytor mellan företagssystem och produktionssystem. Standarden är i sin tur baserad på *Purdue Reference Model* (Williams 1993), vilken ger en hierarkisk bild av produktion och ledning av ett företag.

I ISA-95 identifieras fem nivåer (Figur 6), från process till affärsnivå. På det översta lagret, nivå 4, finns sådana system som kan kopplas till affärsledning[3], förutsättningar för produktion och logistik. Närmast under affärsnivån, på nivå 3, finns produktionsledning. Härifrån styrs och övervakas produktionssystem.[4] På nivå 2 kontrolleras processen genom de kontroll- och mätenheter som återfinns på nivå 1. Den fysiska processen, det vill säga den produktion som utförs, anges som nivå 0.

Nivå 4	Affärsledning och logistik
Nivå 3	Produktionsledning
Nivå 2	Automation
Nivå 1	Sensorer, motorer, ställdon
Nivå 0	Produktionsprocess

Figur 6. De fem nivåerna i ISA-95.

Både ISA-95 och Purduemodellen fokuserar mest på relationen mellan nivå 3 och 4 och ser de underliggande nivåerna mer som traditionell automation.

4.1.3 MESA-modellen

Manufacturing Enterprise Solutions Association (MESA) är en sammanslutning med medlemmar från bland annat tillverkningsindustrin, IT-branschen och

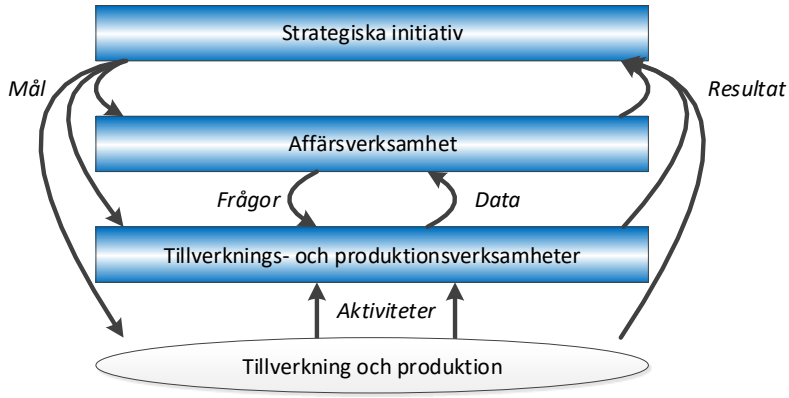
[2] https://www.isa.org/isa95/

[3] Eng. *Enterprise Resource Planning* (ERP)

[4] Eng. *Manufacturing Enterprise System* (MES)/*Manufacturing Operations Management* (MOM)

högskolor. Syftet med MESA är att öka förståelsen för hur IT kan användas för att öka produktivitet och lönsamhet inom industrin.[5]

Inom MESA har flera modeller tagits fram genom åren. Den senaste modellen omfattar fyra nivåer, från en produktionsnivå till en strategisk nivå med affärsmässiga processer (Figur 7).



Figur 7. MESA-modellen.

MESA-modellen illustrerar hur information och data färdas mellan de framtagna nivåerna. På den strategiska nivån sätts mål upp för affärsverksamheten och produktionen. Från dessa nivåer skickas i sin tur resultat tillbaka till den strategiska nivån för att försäkra sig om att målen möts. Skillnader i mål och resultat innebär att en förändring måste göras någonstans i de olika nivåerna för att styra resultaten för att nå de uppsatta målen.

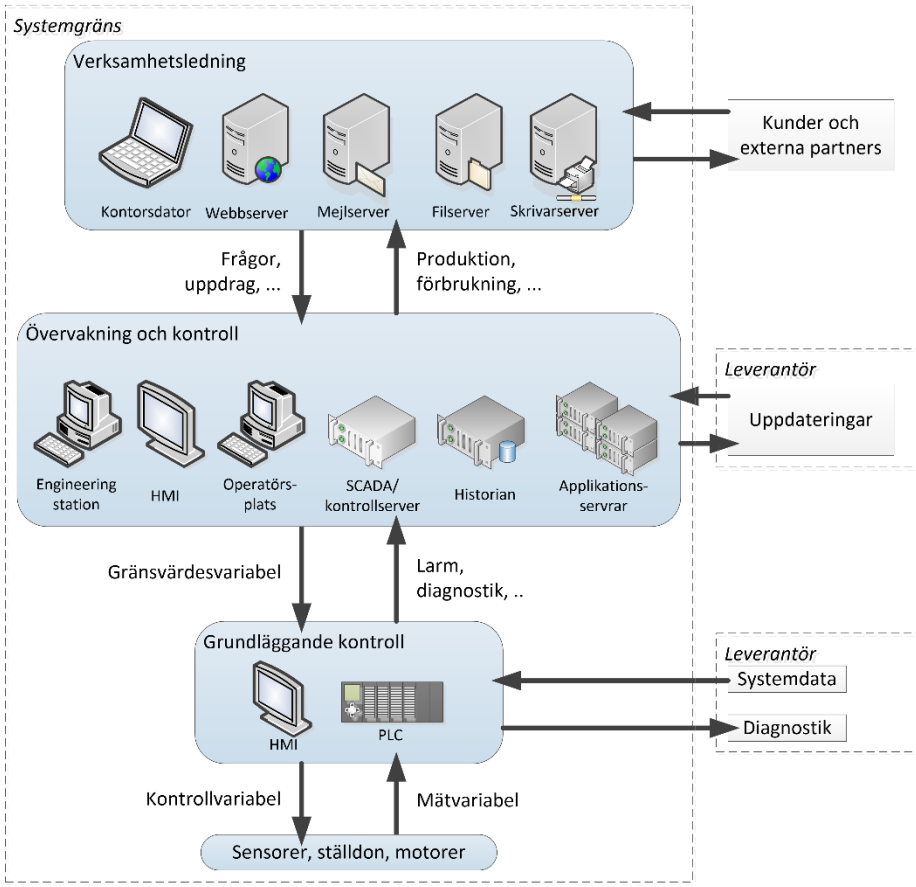
4.2 Dataflöden

Detta avsnitt syftar till att illustrera nödvändig kommunikation mellan olika enheter och delar i ett industriellt informations- och styrsystem. Dessa system och deras komponenter förutsätts ibland vara isolerade från omvärlden, vilket kan vara ett felaktigt antagande då så sällan är fallet (Figur 8).

Den lägsta nivån av kommunikation inom industriella informations- och styrsystem sker generellt mellan en sensor eller motor och en styrenhet. En sensor mäter värden för en viss process och skickar dessa mätvärden till den styrenhet som sensorn är kopplad mot. Denna styrenhet kan i sin tur skicka vidare mätvärdet eller direkt styra processen genom att, baserat på mätvärdet från sensorn, skicka styrsignaler till en motor som är kopplad till processen. Detta sker då automatiskt och är en så kallad sluten slinga (eng. *closed-loop*).

[5] MESA International. http://www.mesa.org/en/index.asp [2017-09-10]

Motsatsen till en sluten slinga, även kallat återkopplingskontroll (eng. *feedback control*), är en öppen slinga (eng. *open-loop*). I en öppen slinga sker ingen direkt styrning utan processen körs konstant under en viss tid. Öppna kontrollslingor används exempelvis av batchprocesser, där resultatet av processen baseras på ett recept.



Figur 8. Informationsflöde.

I större övervakningssystem såsom DCS och SCADA-system skickas sensordata och annan information vidare till en kontrollserver. Denna skickar i sin tur informationen vidare till ett HMI, en Historian och en applikationsserver (se avsnitt 3.4).

DCS skiljer sig något från större SCADA-system som ofta är distribuerade över stora geografiska ytor. En stor skillnad mellan dem är att lokala produktions-system ofta ger en större möjlighet för centraliserad kontroll över en grupp mindre processer. En kontrollserver kommunicerar med dess styrenheter via ett

lokalt nätverk. Servern skickar, automatiskt eller med mänsklig inblandning styrsignaler till, och begär data från, de styrenheter som finns i nätverket. Dessa styr i sin tur sina lokala processmanövreringsenheter baserat på kontrollserver-kommandon och sensorinformation.

Information som genereras inom det industriella nätverket kan också behövas i organisationens kontorsnätverk. Kontorsnätverk och industriella nätverk bör vara logiskt separerade från varandra. Det innebär i sin tur att nätverken måste bryggas för att nödvändig information ska kunna transporteras mellan nätverken. Leverantörer av olika komponenter och system behöver vanligen även en förbindelse in till det industriella nätverket för att underhålla och uppdatera sina komponenter och system. För geografiskt distribuerade nätverk (exempelvis SCADA-system) krävs även en möjlighet att koppla in sig på fältplatser via fjärranslutning då dessa kan vara svåra eller tidskrävande att nå fysiskt.

En skillnad mellan distribuerade övervakningssystem och produktionssystem är den nätverkstyp som är möjlig att använda. För produktionssystem används generellt lokala nätverk (*Local Area Network*, LAN) vilka är snabba och pålitliga. För distribuerade nätverk krävs större nätverk (*Wide Area Network*, WAN), via satellit, telefonlinjer eller radiokommunikation då kommunikationen måste färdas långa sträckor.

Det används en rad olika protokoll för att kommunicera inom industriella informations- och styrsystem. Vilka protokoll som används varierar från anläggning till anläggning och beror även till viss del på typen av anläggning i fråga samt när anläggningen togs i bruk. Av de tolv protokoll som analyserades i Eidenskog och Lindahl (2017) var det endast ett av dessa som uttryckligen hade någon form av inbyggd informationssäkerhetsaspekt. Tio av protokollen hade någon form av säkerhet för drift, men många av dessa förlitade sig dock på underliggande lager (exempelvis TCP/IP eller Ethernet).

5 Analys med hjälp av modeller

För att på ett meningsfullt sätt kunna använda modeller som ett medel för analys krävs det att modellerna skapas ur ett perspektiv som direkt relaterar till verkligheten. Specifikt innebär detta att den arkitektur, de komponenter och de kommunikationsvägar som faktiskt används i verkligheten också representeras i de modeller som återfinns i denna rapport. Det är även viktigt att ta hänsyn till den miljö som industriella informations- och styrsystem idag verkar i, med fokus på de angrepp och intrång som skett de senaste åren. Detta bidrar till en förbättrad möjlighet att resonera kring de risker och sårbarheter som existerar för dessa system, då det kan påvisas vilka sårbarheter som faktiskt utnyttjas av antagonister.

Denna rapport har i kapitel 4 presenterat allmänna modeller, kring vilka det är svårt att diskutera konkreta risker. Detta är dock inte syftet utan istället används modellerna som en utgångspunkt för strukturen av den referensmodell som följer i nästkommande kapitel.

Detta kapitel är ämnat att ge kunskap om de olika exponeringsytor som industriella informations- och styrsystem har. Detta sker i form av beskrivningar av relevanta kommunikationsvägar och säkerhetskomponenter, följt av konkreta exempel på faktiska angrepp mot industriella informations- och styrsystem.

5.1 Exponeringsytor

Alla anslutningsvägar in och ut ur det industriella informations- och styrsystemet är en exponeringsyta som skulle kunna utnyttjas av en potentiell antagonist. För att kunna skydda systemet är det därför viktigt att vara medveten om alla möjliga anslutningsvägar.

Fjärranslutningar används i många organisationers dagliga verksamhet och är ofta nödvändiga för att medarbetare, affärspartners och leverantörer ska kunna utföra sina arbetsuppgifter. Leverantörer använder bland annat dessa anslutningar för att utföra uppdateringar och underhåll av sina egna produkter. Operatörer använder fjärranslutningar exempelvis för att ansluta till understationer. Dessa anslutningar kan dock utnyttjas av potentiella antagonister för att ta sig in i system (Department of Homeland Security (DHS) & Centre for the Protection of National Infrastructure (CPNI) 2010; Verizon 2017). Vanligt använda fjärranslutningstyper som *Virtual Private Network* (VPN) skyddar själva kommunikationen från obehörig avlyssning och manipulation genom att kryptera denna. Skyddsbehovet för dessa anslutningar ligger istället till stor del på de ändpunkter (enheter) som nyttjar anslutningen samt autentisering och åtkomstkontroll för användare som nyttjar ändpunkterna.

Trådlösa lokala nätverk såsom wifi bör kontrolleras och skyddas utförligt då dessa nätverk kan sträcka sig utanför den fysiska plats där de är tänkta att användas. En potentiell antagonist kan även använda sig av en mottagarenhet för att snappa upp svaga signaler och på så sätt få tillgång till nätverket från en avlägsen plats. Det är därför viktigt att nätverket har ett minimiskydd av åtkomst-kontroll i form av ett lösenord. Beroende på vad för typ av kommunikation som flödar i nätverket kan det även vara aktuellt att kryptera trafiken så att obehörig part inte kan läsa kommunikationsinnehåll.

Den attackyta som idag är mest utnyttjad är kontorsnätverket. Som tidigare nämnt har detta nätverk ofta kopplingar in till det industriella kontrollnätverket. Även om det industriella kontrollnätverket inte är anslutet mot några publika nätverk (till exempel internet) så är kontorsnätverket ofta det, vilket innebär att en indirekt kommunikationslinje fortfarande existerar. Ett av de vanligast förekommande angreppssätten via kontorsnätverk, är att på något sätt ta över en dator i kontorsnätverket för att sedan ta sig vidare in till det industriella nätverket (Joyce 2016). För att lyckas med detta krävs det att datorn och användaren i fråga har rättigheterna som krävs att ta sig vidare dit. *Spear phishing*[6] används vanligen som metod i angrepp mot kontorsnätverk, där målet är specifika individer som förväntas ha de nödvändiga rättigheterna.

De incidenter som inträffar i industriella informations- och styrsystem och dess nätverk är inte alltid relaterade till en antagonist. Faktum är att en majoritet av de incidenter som inträffar beror på operatörmisstag, mjukvarufel eller hårdvarufel (Kaspersky 2014). Det är på grund av detta viktigt att inte avgränsa sig för mycket till angrepp som sker utifrån utan även ta hänsyn till de incidenter som är relaterade till misstag och fel. Det finns ett antal åtgärder att tillgå för att minimera uppkomsten av dessa typer av incidenter, bland annat att berörd personal utbildas i de system som används och att denna utbildning kontinuerligt följs upp för att säkerställa att kunskapen inte går förlorad. När det gäller mjukvarurelaterade problem är det viktigt att mjukvara är noga kontrollerad och testad. Det är även viktigt att de uppdateringar som utförs är noga testade innan de implementeras för att undvika att uppdateringen introducerar nya problem. För att skydda sig mot hårdvarurelaterade problem är det viktigt att produkternas funktionella status övervakas och att underhåll utförs kontinuerligt samt efter behov.

Det är en svår uppgift att skydda sig mot incidenter relaterade till misstag eller fel och det är i princip omöjligt att skydda sig till fullo. Det är därför även viktigt att rutiner implementeras för hur sådana incidenter hanteras, för att minimera effekterna av dessa.

[6] Spear phishing är en sofistikerad attack där angriparen lagt ner tid på att skapa ett elektroniskt meddelande, exempelvis ett e-postmeddelande, som riktar sig till ett specifikt offer.

5.2 Exempel på angrepp

I detta avsnitt presenteras ett antal kända angrepp mot industriella informations- och styrsystem. Syftet med detta är att rapportens läsare ska kunna använda beskrivningarna för att diskutera vilka sårbarheter som dessa angrepp nyttjat och hur angreppen i dessa fall skulle kunna stoppas.

5.2.1 Stuxnet

Stuxnet är en datormask innehållande skadlig kod som användes för att sabotera urananrikningscentrifuger i Natanz, Iran. Det som är signifikativt för Stuxnet är dess komplexitet – masken utnyttjade vid angreppet fyra olika *zero-day*[7] sårbarheter, vilket aldrig tidigare skådats; och var även väldigt selektiv i vilka enheter den infekterade. Masken är designad att specifikt angripa en typ av mjukvara från Siemens och riktar sig även mot flyttbara enheter (exempelvis USB-minnen) för att sprida sig.

De enheter som är det slutgiltiga målet för masken är inte anslutna till externa eller publika nätverk såsom internet. För att kunna nå dessa enheter krävs att masken söker efter privata nätverk som den infekterade enheten är en del av. Hittas ett sådant nätverk försöker masken sprida sig inom det nätverket till andra enheter.

Maskens nästa steg är att leta efter projektfiler tillhörande Siemens *WinCC/PCS-7* SCADA-kontrollmjukvara och infektera dessa. Därefter kan masken fånga upp kommunikationen mellan kontrollmjukvaran och Siemens PLC-enheter och installera sig själv på de PLC:er som kommunicerar i det privata nätverket. Stuxnet vill i sin selektivitet endast infektera en viss modell av Siemens PLC (modell S7-300) som har specifika frekvensomvandlingsenheter anslutna. När och om sådana enheter hittats kommer masken att installera sig själv på dessa, för att sedan alternera frekvensen hos urananrikningscentrifugerna genom att periodvis skicka kontrollsignaler från de infekterade PLC-enheterna. I Natanz gjordes detta antingen genom att ställa in en frekvens som fick centrifugerna att skaka okontrollerat och till slut spricka, eller genom att alternera mellan hög och låg frekvens, vilket också resulterade i att centrifugerna sprack eller på annat sätt renderades obrukbara.

Inga varningar nådde fram till kontrollmjukvaran då dessa fångades upp av Stuxnet-masken, således kunde personalen inte göra något för att hindra att centrifugerna tog skada.

[7] Term för en sårbarhet eller fel i programvara, hårdvara eller firmware som är okänd för parten eller parterna som ansvarar för att systemet är uppdaterat. En zero-day kan referera till själva sårbarheten eller till ett angrepp som nyttjar denna sårbarhet.

5.2.2 BlackEnergy 3

Angreppet mot eldistributionen i Ukraina 2015 resulterade i att ca 225 000 abonnenter blev strömlösa i sex timmar. Den skadliga delen av angreppet ägde rum den 23 december 2015 och tog endast minuter att utföra, men senare analys indikerar att intrånget började långt tidigare (Lee, Assante & Conway 2016).

I angreppet nyttjades skadlig kod kallad *BlackEnergy 3*. Den skadliga koden innehåller en samling verktyg som kan användas för att utföra riktade angrepp, primärt mot maskiner som kör diverse versioner av Microsofts operativsystem Windows. Verktygen i BlackEnergy 3 nyttjas bland annat för att skanna nätverk som en infekterad enhet är ansluten till. Detta görs för att inhämta information om nätverket och andra enheter i det. En annan aspekt av informationsinsamling är att stjäla inloggningsuppgifter för att sprida den skadliga koden till andra enheter för att i sin tur komma över mer information samt förse angriparen med kontroll över fler enheter. Ytterligare en komponent av BlackEnergy 3 är en *Killdisk*-mjukvara som kan användas för att radera data från hårddiskar. Detta kan exempelvis användas för att radera data i syfte att försena återhämtningen av systemet samt täcka igen angriparens spår.

Det initiala intrånget som senare resulterade i detta angrepp utfördes genom spear phishing. Denna metod användes för att skicka e-post innehållande Microsoft Office-dokument till utvalda individer. Vad mottagarna inte kunde se var att BlackEnergy 3 var inbäddat i dessa dokument. När dokumenten öppnades installerades och kördes BlackEnergy 3 på datorn. Från datorn kunde det skadliga programmet öppna upp en bakdörr och ansluta till flera olika *Command-and-Control*-enheter (C2). På så sätt fick angriparen tillgång till den infekterade datorn och kunde fjärrstyra denna för övervakning av det lokala nätverket.

Analysen av Lee, Assante och Conway (2016) visar att den första kontakten gjordes mer än sex månader innan själva angreppet. Det är dock troligt att angriparna relativt omgående flyttade lateralt i nätverket och bort från den initiala intrångspunkten för att lättare smälta in och undvika upptäckt.

Efter det initiala intrånget påbörjade angriparna spaning i nätverket och kunde då komma över VPN-anslutningar från kontorsnätverket in till det industriella nätverket. Lee, Assante och Conway (2016) spekulerar i att angriparna stal giltiga inloggningsuppgifter för att nyttja dessa VPN-anslutningar och på så sätt ta sig in i det industriella nätverket. Nästa steg för angriparna var att lära sig det industriella informations- och styrsystemet, hur det fungerade och hur man kan styra det. Från detta utvecklade de troligtvis egna skadliga firmware-uppdateringar för seriell-till-Ethernet-enheter. Dessa enheter tolkar kommandon från SCADA-systemet till de fältstationer där enheterna är belägna.

Själva attacken var välkoordinerad, då man attackerade tre olika organisationer inom 30 minuter. Angriparna tog kontroll över arbetsstationer och HMI samt blockerade användning för personalen. Man använde sedan HMI för att öppna

brytare vilket resulterade i att minst 27 olika fältstationer togs ur bruk och således bröts strömmen för abonnenterna. Samtidigt utförde man sin skadliga firmwareuppdatering, vilket innebar att även om operatörerna återtog kontrollen över arbetsstationerna kunde de inte sätta igång fältstationerna igen. Angriparna påbörjade även en överbelastningsattack via telefon mot elföretagens kundcenter för att abonnenter inte skulle kunna rapportera strömavbrottet. Slutligen använde angriparna KillDisk i Windowsmiljön för att radera *Master Boot Record* (MBR), vilket resulterade i att dessa maskiner blev obrukbara. Dock användes KillDisk i olika utsträckning på olika maskiner, i vissa fall raderades enbart loggar och systemhändelser.

Ingen av dessa komponenter (BlackEnergy 3, KillDisk, den skadliga uppdateringen) hade på egen hand kunnat utföra angreppet. Angreppet var istället ett resultat av direkt manipulation av angriparna på det industriella styrsystemet. De komponenter som användes syftade till att frånta kontroll och försena återställning av systemet medan korrekta och legitima kommandon användes för att stänga av eldistributionen.

5.2.3 CrashOverride/Industroyer

Knappt ett år efter angreppet i Ukraina, 2015 kom nästa angrepp. Den 17 december 2016 bröts strömmen i Kiev i en dryg timme. Angreppet anses av många vara ett storskaligt test eftersom angriparna hade möjlighet att göra mer skada än vad de faktiskt gjorde (Dragos 2017; US CERT 2017). Namnen *CrashOverride* respektive *Industroyer* refererar till samma skadliga kod, men namngavs av två av varandra oberoende utredningar (Dragos 2017 respektive ESET 2017).

Skaparna bakom CrashOverride hade tydligt tagit lärdom av tidigare angrepp. Koden visar ett tillvägagångssätt för att förstå och klassificera kunskaper om industriprocesser för att kunna störa verksamheten, på samma sätt som Stuxnet gjorde. Den skadliga koden utnyttjar *OPC DA*[8]-protokollet för att kartlägga miljön och välja mål på liknande sätt som det skadliga programmet *Havex*[9]. CrashOverride har även ett liknande tillvägagångssätt som angreppet i Ukraina året innan för att förstå funktionalitet hos det utsatta systemet; och för att utnyttja olika delsystem mot varandra. CrashOverride gör allt detta med en bredare och ökad förmåga än de tidigare angreppen.

[8] OLE for Process Control Data Access

[9] Havex är en Remote Access Trojan (RAT) som kopplats till APT-gruppen Dragonfly. Havex är primärt ett informationsinsamlingsverktyg men det har påpekats att det skulle vara relativt lätt för en antagonist att designa om Havex till att inkludera moduler för att åsamka skada i infekterade system (Langill 2014)

Det är inte känt hur CrashOverride introducerades till målsystemet, troligtvis användes någon form av spear phishing. När det skadliga programmet väl tagit sig in på en dator i nätverket installerar det en bakdörr för kommunikation med en kontrollserver (C2) som angriparna använder för att styra programmet. CrashOverride använder sig av en portskanner för att identifiera relevanta mål i nätverket (enheter med högre åtkomsträttigheter) där slutmålet är att först ta sig från kontorsnätverket in i det industriella informations- och styrsystemet och därifrån hitta en enhet med rättigheter att styra RTU:er eller PLC:er. När en sådan enhet hittats och infekterats, skickas legitima styrsignaler till de RTU:er eller PLC:er angriparna vill kommunicera med. Dessa styrsignaler involverar att snabbt alternera mellan att öppna och stänga brytare. Denna händelse triggar i sin tur en självbevarande mekanism där den utsatta RTU:n isolerar sig själv och inte längre tar emot styrning. Detta innebär i praktiken att den fältstation vars RTU blir utsatt stängs ner och således distribueras ingen ström till abonnenter.

Processen beskriven i föregående stycke utgör endast en del i den förmåga som CrashOverride egentligen innehar. Exempelvis finns det i programmet möjlighet att utnyttja gränsöverskridning för värden i syfte att förvirra personal. I praktiken kan detta användas för att skicka felaktig information till operatörer, exempelvis genom att visa att brytare är öppna när de i själva verket är stängda. Denna förvirring innebär ökad tidsfördröjning vid felsökning av systemet och försvårar således återställning.

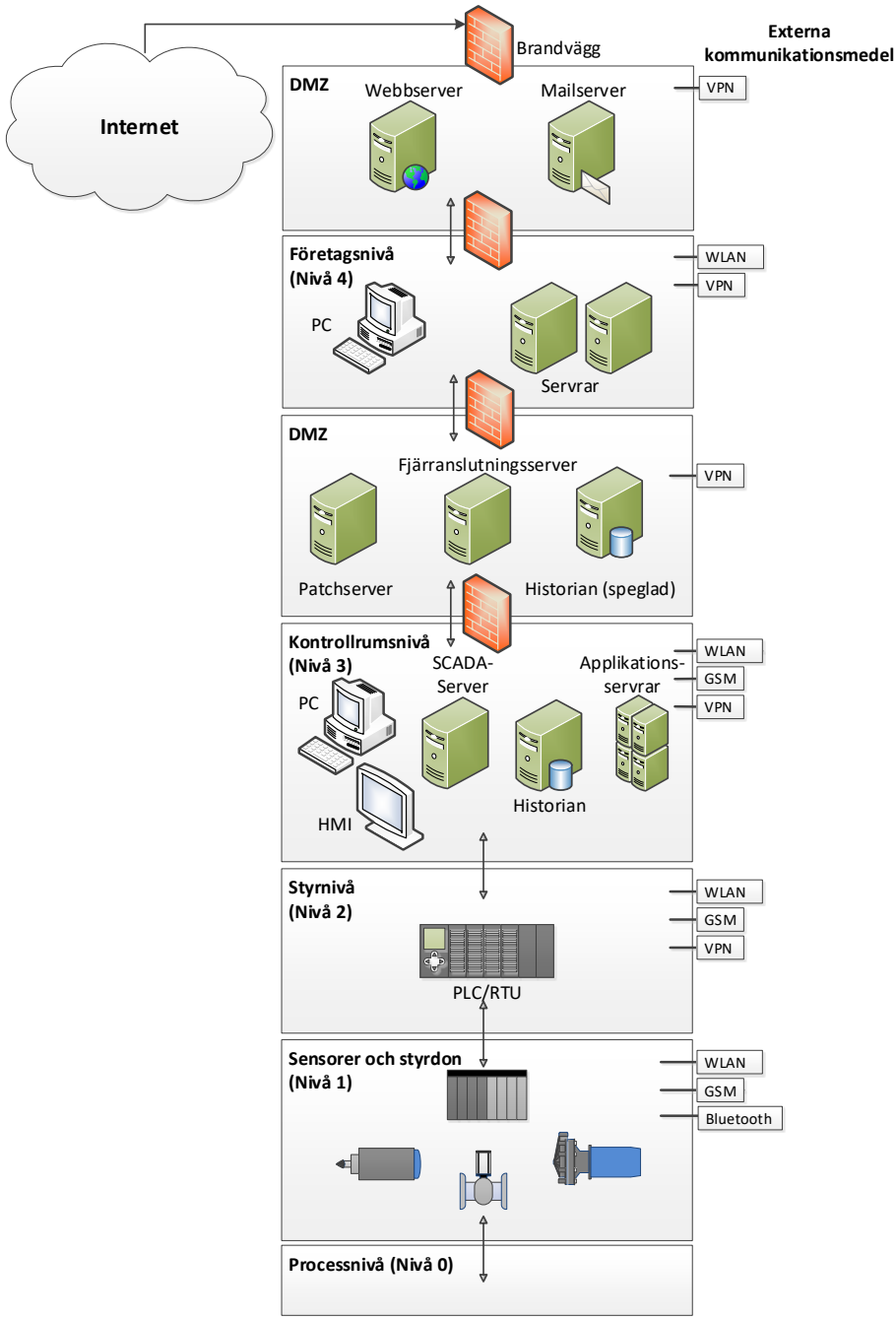
6 Referensmodeller

Det finns flera sätt att beskriva industriella informations- och styrsystem. Hur dessa beskrivs beror på aktuellt fokus. Industriella informations- och styrsystem är på högre abstraktionsnivåer relativt likartade, men skiljer sig därefter beroende på tillämpningsområde. En modell för en teoretisk referensmiljö blir således generisk initialt, men med möjlighet att bli mer detaljerad och specifik efter hand.

Den modell som beskrivs i avsnitt 6.1 belyser olika nivåer i ett industriellt system eller nätverk, kommunikationen mellan dessa nivåer samt anslutningar in i nätverket utifrån. Denna inledande modell är dock relativt generell och det kan därför vara svårt att resonera kring den i en verklig situation. Modellen appliceras därför inom två typfallsexempel (avsnitt 6.2 och 6.3) för att läsaren ska få en förståelse för hur modellen är tänkt att appliceras i olika verksamhetsscenarier. Syftet med detta är dels att ge en förståelse för hur de olika processerna ser ut i dessa typfall och dels att ge en förståelse för hur den inledande modellen kan appliceras i ett konkret exempel. Den framtagna modellen bygger starkt på arkitekturen i ISA-95. Detta val gjordes med bakgrund av att ISA-95 tydligast belyser de områden som är av relevans för att konkret kunna diskutera risker och sårbarheter i industriella informations- och styrsystem.

6.1 Referensmodell

Modellen (Figur 9) illustrerar de olika nivåerna som finns i ett generellt industriellt informations- och styrsystem. Modellen belyser även potentiell kommunikation mellan dessa nivåer.



Figur 9. Föreslagen referensmodell.

Modellen i Figur 9 beskriver ett industriellt nätverk uppdelat i fem olika nivåer samt två buffertnivåer. En *Demilitarized Zone* (DMZ) finns i regel belägen mellan företagsnivån och publika nätverk (internet). En DMZ har till uppgift att förse otillförlitliga nätverk med tillgång till tjänster som behövs utanför interna nätverket utan att ge tillgång till själva nätverket. Mellan företagsnivån och publika nätverk innehåller en DMZ vanligen organisationens webb- och mailservrar samt VPN-gateways och andra tjänster som behöver kunna nås från kontorsnätverket eller publika nätverk.

Nivå 4 innefattar nätverk och komponenter som ligger utanför det industriella nätverket. Primärt i företagsnivån är kontorsnätverket vilket behöver kommunicera med det industriella nätverket för att få tillgång till produktionsdata, historisk data och olika analyser. Den typen av anslutning som används är vanligen VPN eller *Remote Desktop Protocol* (RDP) eftersom kontorsnätverket och industriella nätverket är logiskt åtskilda. Vidare används både VPN och RDP för fjärranslutning till både kontorsnätverket och det industriella nätverket av ingenjörer och leverantörer för att få tillgång till sina delsystem och komponenter, bland annat för att utföra underhåll och uppdateringar.

Mellan Nivå 4 och nivå 3 finns i regel ytterligare en DMZ. Här kan exempelvis det industriella nätverkets Historian speglas i syfte att ge tillgång till information i denna utan att tillåta direkt kommunikation mellan nätverken.

Nivå 3 i modellen visar den översta nivån i det industriella nätverket. Denna nivå representeras av kontrollrummet där övervakning och, i viss mån, styrning av den industriella processen hanteras. På denna nivå finns HMI, SCADA- eller kontrollserver, arbetsstationer, Historian och applikationsservrar. Data som behöver visas utanför det industriella nätverket hämtas inte direkt från de maskiner som opererar här. I stället skickas data till DMZ, som exemplet med en speglad Historian, för att inte ge direkt tillgång till det industriella nätverket. Alla mät och styrsignaler som skickas på någon av de nivåer som tillhör det industriella nätverket hamnar till slut i nivå 3, vilket är nödvändigt för att utföra heltäckande övervakning av processen. Beroende på vilken typ av anläggning man refererar till så ser kommunikationen annorlunda ut. Exempelvis sker kommunikation inom ett DCS vanligtvis via ett LAN medan ett SCADA-nätverk som sträcker sig över stora ytor ofta kräver trådlös kommunikation via WAN eller andra typer av långdistanskommunikation.

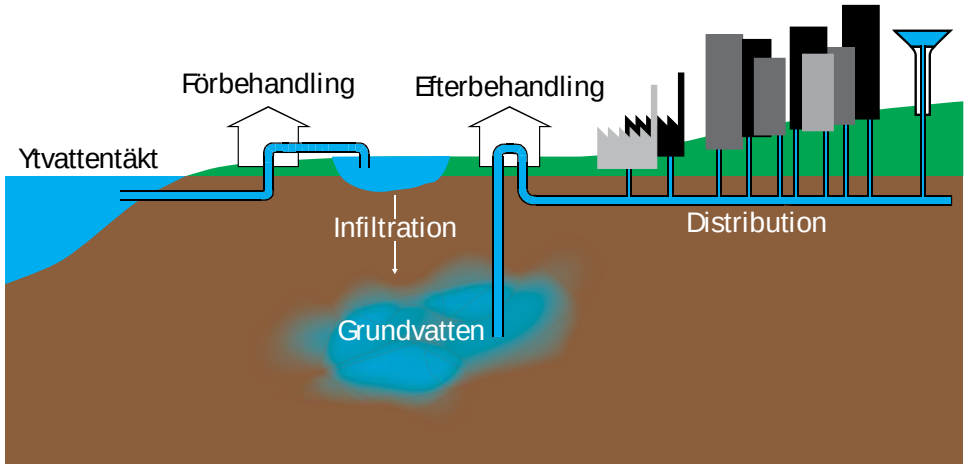
Nivå 2 innefattar kontrollenheter och är även den högsta nivån i ett fristående system. Kontrollenheter i denna mening refererar till exempelvis PLC och RTU. Dessa enheter tar emot signaler från sensorer och ställdon och utför antingen själv styrning eller skickar dessa signaler vidare upp till nästa nivå. I vissa fall innehåller denna nivå även arbetsstationer (som i nivå 3). Dessa arbetsstationer är dock främst riktade till styrning och viss övervakning av enskilda delprocesser. I

nivå 2 används vanliga industriella protokoll för kommunikation och, som nämnt ovan, kan typen av kommunikationsmedel skilja sig mellan olika typer av anläggningar. På nivå 2 och nivå 1 finns även möjlighet att använda trådlösa nätverk för kommunikation på korta avstånd. Exempel på dessa är wifi och Bluetooth. De kontrollenheter som används på nivå 2 kräver periodisk uppdatering och underhåll från leverantörer. Primärt finns det två olika kommunikationsvägar som kan användas för att förse dessa leverantörer med fjärrtillgång till sina delsystem och komponenter utan att utsätta det industriella nätverket i stort för risk. Den ena kommunikationsvägen är att gå via DMZ och en VPN-gateway för att därifrån tunnla ner till de enheter som man behöver tillgång till. Det andra alternativet involverar att leverantören fysiskt befinner sig vid dessa enheter och via en Ethernet-sladd får tillgång till att utföra underhåll och uppdatering.

Nivå 1 representerar den lägsta nivån (undantaget den fysiska processen i nivå 0) i varje industriellt nätverk och innefattar de enheter som är direkt kopplade till den fysiska processen. Dessa enheter består främst av olika typer av sensorer och ställdon. Dessa mäter värden eller utför styrning av en process baserat på kontrollsignaler skickade från nivå 2 eller 3. Som nämnt ovan kan kommunikationsmedel innefatta trådlösa kortdistansmedel, såsom wifi eller Bluetooth, men även trådburen kommunikation används. De protokoll som används för kommunikation i nivå 1 är typiskt *fieldbus* med diverse industriella protokoll, både öppna och proprietära.

6.2 Typfall: Vattenreningsverk

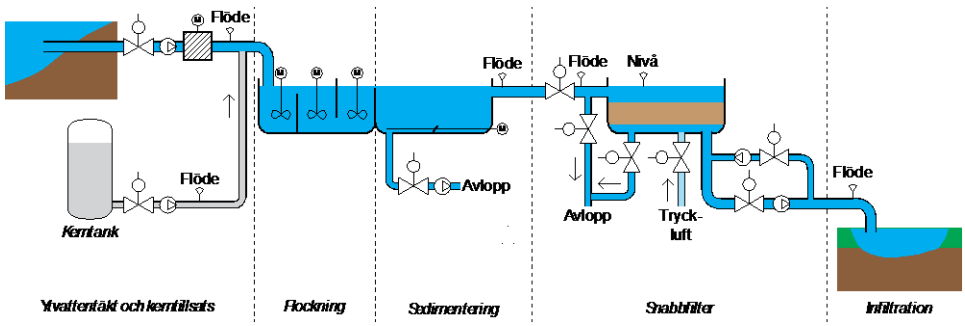
Detta avsnitt beskriver ett hypotetiskt vattenverk för dricksvattenproduktion från en ytvattentäkt. Beskrivningen inkluderar även involverade komponenter och kommunikationen mellan dessa.



Figur 10. Översikt över vattenverk för infiltrerat ytvatten.

Figur 10 visar en översiktlig bild över ett vattenverk där råvattnet tas från en ytvattentäkt, till exempel en sjö. Vattnet genomgår en förbehandling med bland annat flockning och mekanisk rening innan det infiltreras för att skapa grundvatten. Grundvattnet pumpas sedan upp och genomgår en efterbehandling med bland annat pH-balansering och klorering innan det pumpas ut i distributionsnätet.

6.2.1 Förbehandling



Figur 11. Förbehandling av råvatten till infiltration.

6.2.1.1 Nivå 0

Förbehandlingen som renar ytvattnet inför infiltrationen visas i Figur 11. Från ytvattenintaget pumpas vatten genom en finmaskig roterande sil som tar bort grova föroreningar, till exempel vattenväxter. Efter silningen tillsätts flockningskemikalier som används för att klumpa ihop partiklar i vattnet till så kallade flockar i de följande stegen. Typiska flockningskemikalier är vattenglas

(aluminiumsulfat) och soda (natriumkarbonat). Sedan passerar vattnet långsamt flockningsbassängerna där långsamma omrörare blandar vattnet för att flockningskemikalierna ska integreras väl i vattnet. Därefter passerar vattnet en sedimenteringsbassäng där flockarna långsamt sjunker till botten och bildar ett slam. Slammet samlas in av en långsamtgående skrapa på botten av bassängen och pumpas sedan bort. Efter sedimenteringen återstår snabbfiltren där vattnet passerar genom ett metertjockt lager med sand för att fånga upp den lilla rest av flockarna som passerat sedimenteringsbassängerna. Slutligen pumpas det renade vattnet till infiltrationsbassängen där det infiltreras ner till grundvattnet.

Ett vattenverk består normalt sett av flera parallella delflöden där exempelvis flera flockningsbassänger, sedimenteringsbassänger och snabbfilter ger möjligheten att stänga av delar av verket för underhåll och rengöring. Ett exempel på regelbunden rengöring är snabbfiltren som backspolas för att få bort ackumulerade flockar i filtermaterialet.

6.2.1.2 Nivå 1

Den övervakning och styrning som görs på den fysiska processen utgörs bland annat av sensorer som mäter olika värden på delar av processen och motorer som öppnar och stänger olika ventiler. Dessa är i sin tur kopplade till en RTU eller PLC som skickar vidare värdena till kontrollrummet och, baserat på det inkomna värdet, styr processen genom att exempelvis öppna eller stänga en ventil. I förbehandlingsprocessen utgörs övervakning och styrning av sensorer, som mäter flöde och vattennivå, och motorer som styr tillförsel av kemikalier, tryckluft, frekvens på omrörare och skrapa samt pumpning.

6.2.1.3 Nivå 2

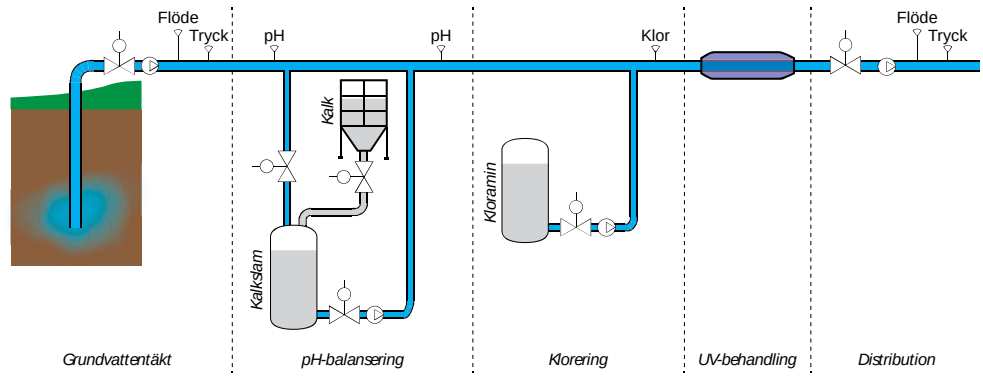
De sensorer, motorer och ställdon som verkar på nivå 1 är kopplade till RTU:er eller PLC:er för att styras och övervakas. Enheterna på nivå 2 utför antingen direkt styrning av processen baserat på de inkomna värdena eller så skickas dessa värden vidare till nivå 3. Detta vattenreningsverk är ett geografiskt distribuerat system och bygger således på en SCADA-arkitektur. Detta innebär i sin tur att majoriteten av all styrning sker automatiskt på nivå 2. RTU:er och PLC:er som utför denna styrning reagerar på inkomna värden. Mer specifikt finns vissa intervaller inprogrammerade i enheten för olika delprocesser. Om ett inhämtat värde då faller utanför ett sådant intervall agerar ansvarig RTU eller PLC genom att exempelvis öppna eller stänga en ventil. I förbehandlingsprocessen är ett sådant exempel att en flödesmätare rapporterar ett för lågt flöde. I respons på detta öppnar den styrande enheten en ventil som kontrollerar vattenflöde och således stiger flödet i ledningen till en korrekt nivå.

De förutbestämda intervallen som finns inprogrammerade för varje enhet sätts via en lokal operatörsstation där en operatör manuellt kan gå in och justera intervallen om så behövs. Processen visas även i ett HMI så att operatörer på plats kan följa processen. Det är dock inte säkert att förbehandlingsprocessen

kräver operatörsövervakning lokalt då processen till stor del är automatiserad. Då finns istället möjlighet att kommunicera med operatörsstationer via VPN-anslutning, på så sätt kan intervallvärden ändras av operatörer på distans.

I regel skickas alla signaler och styrningar vidare från nivå 2 upp till nivå 3 för att möjliggöra övervakning. I vissa fall är detta dock inte möjligt i samma utsträckning då kontinuerlig kommunikation kan bli för kostsam. Det bättre alternativet blir då att istället enbart skicka de mätvärden som resulterar i att en styrning behöver utföras samt periodvisa uppdateringar. Eftersom detta är ett distribuerat SCADA-nätverk krävs det en kommunikationstyp som klarar av att färdas långa sträckor på rimlig tid exempelvis via telenät eller satellit.

6.2.2 Efterbehandling



Figur 12. Efterbehandling av grundvatten till distribution.

6.2.2.1 Nivå 0

Efterbehandlingen startar med att grundvattnet pumpas upp ur djupborrade brunnar. Sedan tillsätts uppslammat kalk för att balansera pH-värdet i vattnet för att det inte ska vara korrosivt mot vattenledningsnätet. Därefter tillsätts en liten mängd klor för att minska risken för bakterietillväxt i ledningsnätet. Det sista reningssteget är ett UV-behandlingsaggregat som eliminerar en stor del av de bakterier, virus och parasiter som kan tänkas finnas i vattnet. När vattnet har passerat UV-filtret är det färdigt att pumpas ut i ledningsnätet.

6.2.2.2 Nivå 1

På samma sätt som i förbehandlingen övervakas och styrs denna process med hjälp av sensorer, motorer och ställdon. I efterbehandlingsprocessen finns exempelvis sensorer som mäter pH-värdet i vattnet. Motorer styr ventiler för tillsättning av kalkslam och klor. Det finns även sensorer för att mäta flödet och trycket i efterbehandlingsröret. Dessa värden regleras efter behov för att försäkra

sig om att trycket eller flödet i efterbehandlingsröret inte ligger på nivåer som kan skada vattenledningsnätet eller vattenreningsverket.

6.2.2.3 Nivå 2

Inkomna pH-värden från sensorer bestämmer om tillsättning av kalkslam behövs. Rapporteras ett pH-värde som faller utanför det förutbestämda intervallet påbörjar ansvarig RTU eller PLC styrning för att reglera detta genom att starta en motor som öppnar ventilen för tillsättning av kalkslammet. Efter denna tillsättning rapporteras ytterligare ett pH-värde för att se om regleringen gett tillräcklig effekt. Nästa steg är att via en ventil tillsätta klor. Denna ventil styrs av en motor som i sin tur styrs av en RTU eller PLC. Efter tillsättningen mäts mängden klor för att se om mängden är inom tolererade värden. Slutligen pumpas vattnet vidare för distribution.

6.2.3 Distribution

När efterbehandlingsprocessen har slutförts ska vattnet distribueras till kunder. Vatten produceras dock inte på begäran och kräver således lagring, vilket ofta sker i vattentorn.

6.2.3.1 Nivå 0

Vid efterbehandlingens slutskede pumpas vattnet vidare direkt ut till kunder, men också till vattentorn för lagring. Då vattnets distributionsrör täcker stora ytor krävs det ett högt tryck i rören för att vattnet inte ska stanna av. Vidare sker vattenlagring ofta i vattentorn som är belägna över marknivå, vilket medför behov av högtryckspumpar. Vatten måste även levereras under olika nivåer av tryck för olika kunder och för detta ändamål används tryckstegringspumpar.

En annan viktig egenskap hos distributionsnätet är att det måste vara en sluten process för att försäkra sig om att ingen yttre påverkan, medveten eller omedveten, kan kontaminera vattnet eller orsaka läckage. I praktiken innebär detta att majoriteten av vattenledningar är nedgrävda under marken och att synliga delar härdas mot yttre fysisk påverkan och sabotage.

Identifiering och spårning av läckage är viktigt i distributionsnätet. Läckor kostar inte bara i förlorade intäkter utan kan även orsaka skada på egen utrustning eller kunders egendom. Det är därför nödvändigt att snabbt kunna identifiera läckage för att minimera konsekvenserna.

6.2.3.2 Nivå 1

Distributionsprocessen består till stor del av högtryckspumpar, ventiler och olika sensorer som mäter tryck, pH-värde, kontamination och vattennivå.

6.2.3.3 Nivå 2

Precis som i förbehandling och efterbehandling är det RTU:er eller PLC:er som styr och samlar in data från enheterna i nivå 1. Dock är distributionsnätet väsentligt större än föregående processer eftersom vattnet nu ska distribueras till kunder och således behöver färdas längre sträckor. Detta innebär i sin tur att de RTU:er, PLC:er, pumpar och sensorer som samlar in data från och styr processen också är distribuerade över större ytor. Detta innebär däremot inga större svårigheter med att använda samma typ av kommunikation mellan nivå 1 och nivå 2 som i de andra delmomenten. Istället innebär det att fysisk tillgång måste möjliggöras, men också regleras. För att möjliggöra fysisk tillgång placeras de styrande enheterna i nivå 2 i låsta rum eller små byggnader i anslutning till de rör där vattnet flödar. I dessa lokaler finns förutom styrande enheter även operatörsstationer och HMI för delprocessen. Detta underlättar styrning av specifika enheter då man kan ansluta till en operatörsstation via fjärranslutning och på så sätt ändra intervallvärden.

6.2.4 Nivå 3 Kontrollrummet

De mätningar och styrsignaler som skickas från nivå 2 går vidare till nivå 3 och kontrollrummet. Genomströmningen i det kommunikationsmedium som används är ofta relativt låg, vilket innebär att det inte är hållbart att skicka och ta emot realtidsdata. Statusuppdateringar sker istället med jämna mellanrum samt för varje styrning som utförs från nivå 2 på nivå 1.

Inkommen data till kontrollrummet hamnar först i SCADA-servern som i sin tur reläar data vidare till ett HMI och till en Historian som lagrar alla data och alla styrningar. Data skickas även vidare till en applikationsserver som hanterar status och förväntat underhållsarbete för varje enskild enhet i nätverket. HMI:t visar aktuella data för processer i ett grafiskt gränssnitt. Detta gränssnitt är punkten där övervakning övergår från automation till mänsklig inblandning. I kontrollrummet sitter en eller flera operatörer och övervakar olika delprocesser, processen i sin helhet och distributionen av vattnet. I kontrollrummet ges även möjlighet att koppla upp sig på de distribuerade operatörsstationer som finns placerade runt om i de olika delprocesserna. Genom denna uppkoppling kan man sedan styra processen genom att ändra olika gränsvärden – eller i vissa fall utföra direkt styrning av en delprocess.

I kontrollrummet finns även nödstopsfunktioner (eng. *kill switch*) för alla delprocesser, processen i sin helhet, samt för distributionen.

6.2.5 Nivå 4 Företagsnivå

Som tidigare nämnts behöver ofta kontorsnätverket tillgång till data som genereras och lagras i det industriella nätverket (nivå 3). Att förse enheter i kontorsnätverket med direkt tillgång till det industriella nätverket är dock inte att rekommendera då detta innebär en onödig exponering av kontrollnätverket. Istället används i regel en DMZ som ett mellanlager där en databasserver placeras, innehållande de data som behövs i kontorsnätverket. Detta innebär att en begäran att få data kommer från kontorsnätverket till DMZ och databasservern. Databasservern skickar i sin tur tillbaka relevant data. Om databasserven däremot inte har de begärda data skickar serven i sin tur en egen begäran in till det industriella nätverket och den Historian som ligger där, som svarar med att skicka tillbaka efterfrågade data. Samma resultat kan erhållas genom att använda en VPN-gateway i DMZ som i sin tur sköter kommunikation med Historian. För verksamheten kring ett vattenreningsverk är de data som kontorsnätverket behöver framförallt kvalitet och kvantitet av vatten som pumpas ut och används samt vattenlagringsnivåer.

Kontorsnätverket är ett traditionellt IT-system och påverkas således av samma hot och sårbarheter som dessa gör. Verksamheten har externa tjänster, och av samma anledning som man inte vill ge direkt tillgång till det industriella nätverket från kontorsnätverket vill man inte heller ge utomstående nätverk tillgång till det interna kontorsnätverket. Därför placeras det även en DMZ utåt mot internet och andra nätverk, så att kunder kan få tillgång till tjänster utan att få tillgång till det interna nätverket. I DMZ finns typiskt webbserver, applikationsserver, databasserver, mailserver samt VPN-gateway. Inne i själva kontorsnätverket finns motsvarigheter för dessa som ansvarar för att ta emot och skicka tillbaka data till DMZ på begäran.

Precis som i andra organisationer kräver olika arbetsroller olika tillgång till information för att utföra sitt arbete. Därför finns det restriktioner för vilka enheter som kan begära och hämta data från det industriella nätverkets DMZ.

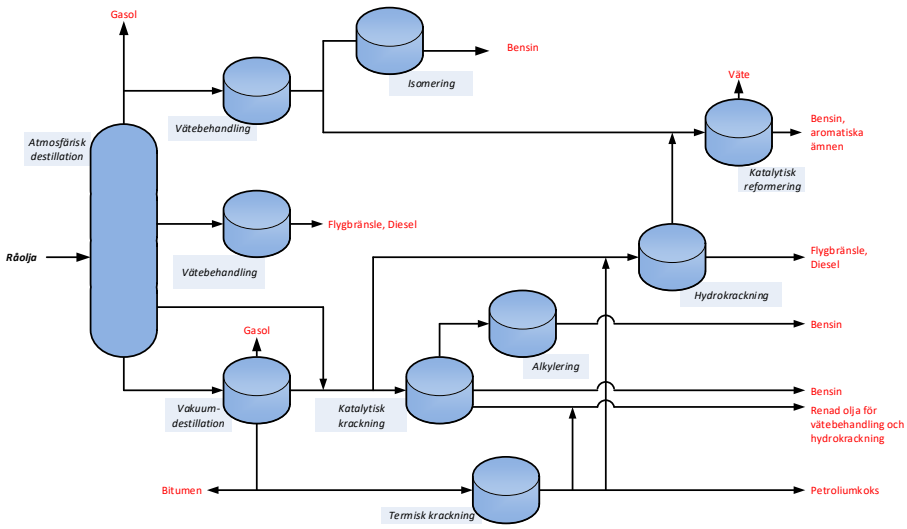
Det finns vissa arbetsroller som kräver tillgång till det industriella nätverket på distans. För att lösa detta används ofta VPN eller andra former av fjärranslutning. Viktiga aspekter gällande VPN-anslutningar in i det industriella nätverket inkluderar förutom stark autentisering av användare även strikt åtkomstkontroll. Med strikt åtkomstkontroll avses att användare endast bör ges tillgång till de enheter och tjänster denne behöver för att utföra sitt arbete samt att en användare aldrig bör ha högre behörighet via fjärranslutning än vad denne har lokalt på sin arbetsplats.

6.3 Typfall: Oljeraffinaderi

Detta avsnitt beskriver processerna i ett hypotetiskt oljeraffinaderi. Beskrivningen inkluderar även involverade komponenter samt kommunikation mellan dessa.

Framställning av oljebaserade produkter som bensin och diesel görs i raffinaderier. Alla framställningssteg sker inom raffinaderiet och har en hög grad av automation samt flera delsteg som kan vara hälsovådliga för människor att utföra. Den avgränsade ytan som raffinaderiet utgör och behovet av en central övervakning, men med lokalt självkontrollerande delar, gör ett destilleri till ett exempel där DCS kan användas.

Raffineringsprocessen från råolja till oljeprodukter genomgår upp till tre processteg: *raffinering*, *förädling* och *rening*.



Figur 13. Generisk vy av ett oljeraffinaderi.

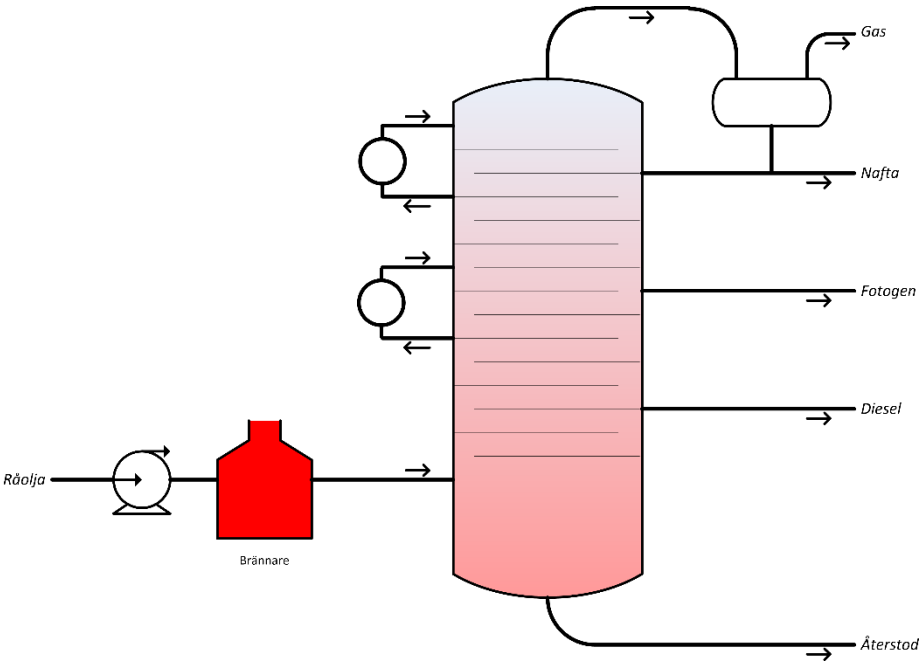
6.3.1 Raffinering

Råolja raffineras i flera steg för att skapa slutprodukter såsom bensin, diesel, flygbränsle och gas. För specialiserade slutprodukter kan även viss raffinering göras på andra raffinaderier.

6.3.1.1 Nivå 0

Raffinering sker primärt i två steg. Först separeras råolja genom *atmosfärisk destillation* till olika ämnen (olika molekyllängder). Restprodukten (Long residue) från destillationen innehåller fortfarande lättare gaser vilka genomgår en

andra destillation, en så kallad *vakuumdestillation*. Råolja pumpas från sin lagringsplats till en brännare som värmer upp råoljan. Därefter pumpas oljan in i destillationskolonnen. Genom destillationen utvinns olika oljeprodukter vilket medför att temperaturkontroll är mycket viktigt under destillationsprocessen. För att öka effektiviteten i destillationen pumpas även kondenserad vätska mellan olika nivåer i destillationskolonen, så kallad *pump-around*.



Figur 14. Principbild av atmosfärisk destillation.

En av de produkter som utvinns under den atmosfäriska destillationen är nafta. Nafta är en viktig komponent för att exempelvis framställa bensin. Den nafta som erhålls vid destilleringen är dock för lågoktanig och behöver förädlas innan den kan bli bensin. Ett sådant förädlingssteg är naftareformering.

6.3.1.2 Nivå 1

Denna nivå är den del av systemet som är närmast kopplat till den fysiska processen. Nivå 1 innehåller med andra ord alla mätinstrument och styrningskomponenter som används för att övervaka och styra processen. Dessa instrument och komponenter utgörs främst av olika sensorer, motorer och ställdon. Som beskrivet i föregående avsnitt är temperatur en viktig mätpunkt för raffineringsprocessen. Denna mätning utförs automatiskt av sensorer som i sin tur vidarebefordrar inhämtade temperaturvärden till en PLC eller RTU i nivå 2. Andra sensorer mäter exempelvis flödet av den olja som pumpas eller tryck i ledningar. I nivå 1 finns även motorer och ställdon som exempelvis öppnar och

stänger ventiler eller pumpar kondenserad vätska, för att hantera flödet av råolja och temperatur i brännaren.

En annan väldigt viktig kontrollpunkt är läckage då en okontrollerad antändning av någon av de produkter som hanteras i raffinaderiet kan få katastrofala konsekvenser och i värsta fall kosta människoliv. Upptäckt av läckor sker med hjälp av flera olika typer av sensorer. Exempelvis kan en läcka indirekt upptäckas genom att flödet i en ledning utan klar anledning sjunker. Ett annat exempel är gassensorer som placeras utanför gränsen för den fysiska processen och som reagerar på gasmolekyler i luften.

6.3.1.3 Nivå 2

Nivå 2 innehåller de enheter som har kapacitet att utföra direkt styrning av den fysiska processen genom att skicka styrsignaler till underliggande instrument i nivå 1. Denna kapacitet utgörs till största del av RTU:er och PLC:er då dessa har kapacitet att utföra styrning av sina olika delprocesser baserat på förutbestämda intervallvärden.

RTU:er och PLC:er tar emot mätvärden från olika sensorer och reagerar om värdena faller utanför ett fördefinierat intervall. Alla mätningar som tas emot och styrningar som görs av en RTU eller PLC skickas alltid vidare till nivå 3 och kontrollrummet. Detta syftar till stor del att förse kontrollservern och operatörerna i kontrollrummet med realtidsinformation för att på ett effektivt och säkert sätt kunna styra och övervaka hela produktionsprocessen i raffinaderiet.

6.3.2 Förädling och rening

Endast en mindre del av den destillerade råoljan omvandlas till lättare produkter. Behovet av lättare produkter såsom gas och bensin är dock stort vilket gör att dessa gaser utvinns ur det tyngre restmaterialet (short residue). Slutligen renas produkterna genom *vätebehandling* där svavel avlägsnas.

6.3.2.1 Nivå 0

Den huvudsakliga processen för förädling kallas för *krackning* och innebär att längre molekylkedjor bryts ner till kortare, och därmed lättare, molekylkedjor. Metoderna för krackning kallas för *termisk krackning*, *katalytisk krackning* och *hydrokrackning*.

Det är också möjligt att sätta samman för korta molekylkedjor till önskad längd genom *katalytisk reformering* samt omstrukturera molekyler genom så kallad *alkylering*.

Inom ett raffinaderi tillverkas även produkter som används i andra delar av processen. *Isomering* omvandlar linjära molekyler till grenade molekyler, vilket medför ett högre oktantal som kan användas i bensin eller för alkylering. I

katalytisk reformering separeras de aromater som tagits fram vid (nafta)reformeringen. En restprodukt från denna process är vätgas, vilken används i reningsprocesser.

Renade produkter förvaras i lagringstankar medan andra produkter skickas till blandtankar innan de kan lagras som slutprodukter. I blandtankar skapas exempelvis rätt oktantal för bensin.

6.3.2.2 Nivå 1

På samma sätt som för raffineringsprocessen finns i denna nivå 1 sensorer, motorer och ställdon som kontrollerar och övervakar den fysiska processen. Viktiga mätvärden för förädling och rening är bland annat flöde, tryck och temperatur. För blandningsprocessen är det exempelvis viktigt att kontrollera att korrekta mängder blandas för att skapa rätt produkt. För att övervaka detta är det därför viktigt att kontrollera flödet av de olika ämnen som tillsätts i blandningen. Flödet och trycket mäts av olika sensorer och påverkas i sin tur av motorer som styr pumpar i anslutning till ledningarna.

Kontroll av läckage är, precis som för raffinering, även viktigt för förädlings- och reningsprocessen.

6.3.2.3 Nivå 2

PLC:er och RTU:er tar in och reagerar på de värden som rapporteras från underliggande sensorer. En reaktion för förädlings- och reningsprocessen kan vara att RTU eller PLC skickar en styrsignal till en motor att sänka pumpningsfrekvensen för att minska trycket i ledningen. Detta används exempelvis för att kontrollera att blandningen i tankarna följer rätt recept.

6.3.3 Nivå 3 Kontrollrummet

I ett DCS är det fullt möjligt att ha realtidsuppdateringar av mätvärden då anläggningen och alla dess komponenter är lokalt belägna och kommunikationen således inte behöver färdas långa sträckor. Alla de värden och styrsignaler som skickas från lägre nivåer hamnar till slut i kontrollrummet.

I kontrollrummet finns en kontrollserver, ett HMI, en Historian, flera applikationsservrar och operatörsstationer. Kontrollservern tar emot alla data från de lägre nivåerna och reläar dessa vidare till Historian som lagrar alla mätvärden och styrsignaler. HMI:t visar de aktuella värdena och status för varje process. Kontrollservern skickar även vidare data till applikationservrarna så att dessa ska kunna utföra statusanalyser för varje enhet i nätverket.

Kontrollservern skickar inte bara vidare data till andra enheter i kontrollrummet, den har även möjlighet att överskådligt styra alla delprocesser i nätverket. Detta

kan göras automatiskt eller med inblandning via en operatörs interaktion på plats i kontrollrummet.

I kontrollrummet sitter flera operatörer och övervakar de olika processerna, precis som i föregående typfall. De olika delmomenten i tillverkningsprocessen i ett raffinaderi, och i ett DCS generellt, är till stor del oberoende av varandra, i den mening att den enda hänsyn som tas till andra processer är in- och utmatning. Det är till exempel viktigt att inte mata ut mer än vad nästa delprocess för tillfället kan hantera. I ett DCS, och i ett raffinaderi, finns därför processindelad övervakning i form av säkerhetszoner med en process i fokus för varje zon i kombination med de in- och utmatningar och andra beroenden som finns till andra delprocesser.

De olika delprocesserna är till stor del självstyrda, men det är kontrollservern som kontrollerar och styr den övergripande processen. Denna styrning sker automatiskt av kontrollservern eller via mänsklig interaktion av operatörer i kontrollrummet.

6.3.4 Nivå 4 Kontorsnätverket

Precis som i det föregående typfallet är kontorsnätverket i detta typfall ett traditionellt IT-system och påverkas av samma hot och sårbarheter som andra kontorsnätverk.

Kontorsnätverket behöver kommunicera med det industriella nätverket för att få ut värdefull verksamhetsinformation. För ett raffinaderi är denna information främst produktionsvolym, innehav av råolja och distributionsrelaterade ärenden.

Som beskrivet i det föregående typfallet, behöver olika arbetsroller olika åtkomsträttigheter till delar av system och nätverk. Detta gäller för de allra flesta typer av organisationer och är således inte unikt för industriella informations- och styrsystem. Däremot är det synnerligen viktigt att dessa rättigheter hanteras för industriella informations- och styrsystem då dessa system hanterar fysiska, och ofta känsliga, processer med potential att påverka det fysiska rummet.

Fjärranslutningar, ofta i form av VPN, används av operatörer och kontorsanställda såväl som av leverantörer och affärspartners. Dessa anslutningar och vem som har rätt att ansluta måste strikt regleras av organisationen, inte minst om leverantörer och affärspartners är externa parter. DMZ och VPN-gateways spelar en viktig roll då det genom dessa kan ges tillgång till information och data från det industriella nätverket utan att det ges möjlighet att via anslutningen påverka de enheter eller processer som finns där.

7 Diskussion

Målet för denna rapport var att ta fram en teoretisk referensmiljö i form av en modell mot vilken det går att resonera kring risker, hot och sårbarheter avseende industriella informations- och styrsystem. Detta i syfte att öka förståelsen och förenkla kunskapsspridningen inom området utan att äventyra informationssäkerheten.

Referensmodellen bygger på en vedertagen arkitektur och den beskrivs på en relativt hög abstraktionsnivå. Detta bidrar positivt till modellens relevans eftersom den valda abstraktionsnivån möjliggör att majoriteten av industriella informations- och styrsystem kan beskrivas enligt denna modell. I vissa fall bör en komplettering ske, vilket är möjligt. Detta påvisas genom de två typfallsexempel som beskrivs i avsnitt 6.2 och 6.3, som även visar att olika verksamheter med olika typer av system kan beskrivas utifrån samma modell. Således kan risker, hot och sårbarheter avseende industriella informations- och styrsystem, som beskrivs i kapitel 5, diskuteras på både en generell nivå och en detaljerad nivå med stöd av en referensmodell som beskrivs i kapitel 6.

Trots den relativt höga abstraktionsnivån och mångsidigheten hos modellen behöver potentiella användare inneha en viss nivå av domänkunskap gällande industriella informations- och styrsystem för att nyttja modellen till fullo. Rapportens inledande kapitel (1–4) kan användas för att tillse viss domänkunskap, även om dessa kapitel inte är uttömmande.

Referenser

Department of Homeland Security (DHS) & Centre for the Protection of National Infrastructure (CPNI) (2010). *Configuring and Managing Remote Access for Industrial Control Systems*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf

Dragos (2017). *Crashoverride - Analysis of the Threat to Electric Grid Operations*. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Eidenskog, D. & Lindahl, B. (2017). *Industriella protokoll i Sverige - En översikt över protokoll inom industriella informations- och styrsystem i kritisk infrastruktur* (FOI-R--4438--SE). Stockholm: Totalförsvarets forskningsinstitut

ESET (2017). *Industroyer: Biggest malware threat to critical infrastructure since Stuxnet*. Bratislava: ESET.

Galloway, B. & Hancke, G.P. (2013). Introduction to Industrial Control Networks. *IEEE Communications Surveys & Tutorials*, 15(2), ss.860 – 880. doi: 10.1109/SURV.2012.071812.00124

Joyce, R. (2016). Disrupting Nation State Hackers [video]. *USENIX Enigma Conference*. San Francisco (CA), USA 25-27 januari 2016. https://www.youtube.com/watch?v=bDJb8WOJYdA [2017-12-14]

Kaspersky (2014). *Industrial Security. Cyberthreats to ICS systems - You Don't Have to be a Target to Become a Victim*. https://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf

Langill, J.T (2014). *Defending Against the Dragonfly Cyber Security Attacks.* St. Louis: Belden. http://www.emrsolutions.ie/wp-content/uploads/2014/12/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

Langner, R. (2013). *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Hamburg: The Langner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lee, R.M., Assante, M.J. & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case*. Washington D.C.: E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Stouffer, K., Pillitteri, V. Lightman, S. Abrams, M. & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (SP 800-82). 2 uppl., Gaithersburg: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Thuen, C. (2016). *Commonalities in Vehicle Vulnerabilities*. Seattle: IOActive. https://ioactive.com/pdfs/Commonalities_in_Vehicle_Vulnerabilities_WP.pdf

US-CERT (2017). Alert (TA17-163A) *CrashOverride Malware*. 12 juni. https://www.us-cert.gov/ncas/alerts/TA17-163A (2018-11-26)

Verizon (2017). *2017 Data Breach Investigations Report*. 10 uppl. https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Williams T. J. (1993). The Purdue Enterprise Reference Architecture. I *IFAC Proceedings Volumes, 12th Triennal Wold Congress of the International Federation of Automatic control*. 26(2). Sydney, Australien 18-23 juli, ss. 559–564. doi: 10.1016/S1474-6670(17)48532-6.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se