Arbetsmiljöfonden

SAMMANFATTNING 1662

Säkerhet i industrin

REKOMMENDATIONER OCH ANVISNINGAR FÖR PROGRAMMERBARA ELEKTRONISKA STYRSYSTEM

I en ökande omfattning används elektroniska styrsystem för att övervaka och styra processer inom industrin. Samtidigt tenderar funktionerna och därmed programvaran i styrsystemen att bli alltmer komplexa. På så sätt ökar också riskerna för störningar inom systemet.

Mot den bakgrunden har Föreningen för Industriell Elteknik, FIE, arbetat fram en handbok inom området. Projektet är ett samarbete mellan olika specialister inom svensk process- och kraftindustri, samt konsulter och tillverkare/leverantörer av styrsystem.

Till grund för handbokens rekommendationer ligger en störningsanalys, som omfattar såväl maskin- som programvara och människa-maskinfunktionen.

För innehållet svarar
Erik Lundquist
Föreningen för Industriell Elteknik, FIE,
Box 8133,
104 20 Stockholm,
telefon 08-657 12 06.

BAKGRUND OCH SYFTE

Elektroniska styrsystem används i ökad omfattning för att övervaka och styra processer inom industrin. Samtidigt tenderar funktionerna och därmed programvaran i styrsystemen att bli alltmer komplexa. På så sätt ökar risken för störningar inom systemet.

Mot den bakgrunden har Föreningen för Industriell Elteknik, FIE, i ett samarbetsprojekt mellan specialister inom svensk processindustri, kraftindustri, konsulter och tillverkare/leverantörer av styrsystem arbetat fram en handbok inom området programmerbara elektroniska styrsystem.

Handboken är avsedd att vara ett hjälpmedel i säkerhetsavseende för alla som ansvarar för eller arbetar med styrsystem och dess nyttjande vid projektering, drift och underhåll. Den rekommenderar åtgärder mot säkerhetsrisker för såväl person som maskin och process, men ger också organisatoriska rekommendationer.

Handboken vänder sig till följande målgrupp:

- beslutsfattare
- projektledare
- processtekniker
- projektörer och konstruktörer
- installatörer och idrifttagare
- operatörer och driftspersonal
- underhållspersonal.

Av praktiska och ekonomiska skäl kan handboken beröra endast en begränsad typ av styrsystem. Som grund för studien och rekommendationerna ligger ett större integrerat operatörsbaserat styrsystem. Men oavsett industrins typ och storlek kan handboken vara ett hjälpmedel där tillämpliga delar av rekommendationerna kan väljas ut. För mindre styrsystem gäller i princip liknande rekommendationer som för större. En anpassning får göras till det egna projektets behov.

I ett integrerat styrsystem är de eltekniska och elektroniska komponenterna sammansatta till funktioner för processövervakning och -påverkan. Vid projektering och konstruktion berörs specialister från skilda teknikgrenar.

För att de av de processansvariga önskade funktionerna ska förverkligas på rätt sätt, vara säkra och uppfylla önskemålen måste nära samverkan ske mellan teknikgrenarna. Viktigast är naturligtvis personsäkerheten som aldrig får ifrågasättas och som visserligen regleras av lagar och föreskrif-

ter, men som detaljerat måste beaktas från säkerhetssynpunkt vid projektering och konstruktion.

PROJEKTARBETET

Projektarbetets mål var att utarbeta rekommendationer för säkrare systemuppbyggnad, samt drift och underhåll av styrsystem. Arbetet bedrevs i projekt- och arbetsgrupper om tillsammans ca 40 specialister.

Till grund för rekommendationerna ligger en störningsanalys. Den omfattar såväl maskinvara som programvara och människa–maskinfunktion.

Styrsystemomfattningens gränssnitt inbegriper på ingångssidan givare och signaldon och på utgångssidan den signal som påverkar ställdon av något slag. Likaså innefattas kringutrustning såsom matningsdon, skrivare och operatörsutrustning. Mellan ingångssida och utgångssida återfinns interface och den programmerbara delen.

HANDBOKENS INNEHÅLL

Grundläggande definitioner

En "störning" inom definierat styrsystem kan härledas från:

- Onormala funktioner och /eller data som avviker från specifiserade egenskaper eller värden.
- Felaktigheter i utförande alltifrån planering till idriftsättning eller felaktigt handhavande vid drift och underhåll.

Störningen kan ge upphov till en störeffekt som kan uppträda i program- eller maskinvara. Störeffekten kan resultera i en säkerhetskonsekvens i form av person–maskin- eller processrisk. Sålunda kan styrda objekt, som är anslutna till styrsystemet, anta oönskade tillstånd som i sin tur kan skada person eller påverka maskin, process eller miljö med ekonomiska konsekvenser som följd.

I handboken ges rekommendationer för att motverka sådana följder.

Säkerhetsbegreppet

Styrsystemet måste vara så konstruerat att det inte ger upphov till säkerhetsrisker i den process det är ägnat att styra. Här beskrivs vad som avses med skilda typer av *bristande säkerhet*:

- *Bristande personsäkerhet* så att personer kan komma till skada direkt eller indirekt. Direkt kan vara obefogade rörelser eller obefogad spänningssättning. Indirekta skador kan uppstå genom att processen påverkas felaktigt så att den i sin tur utgör en källa till risk för personskador.
- *Bristande maskinsäkerhet* som innebär skador på maskiner kan resultera i ekonomiska konsekvenser.
- *Bristande process-, miljö- och driftssäkerhet* innebär försämrad kvalitet på produkten, dålig verkningsgrad eller skador på natur eller miljö.

Vid planering och projektering av styrsystem bör först en störningsanalys utföras som grund för *säkerhetsanalysen*. Den ska utgå från processens krav och felrisker och studera hur anläggningen ska fungera i såväl normala som störda driftsfall.

Säkerhetsanalysen ligger till grund för de kravspecifikationer som säljaren/leverantören har att ta hänsyn till vid konstruktion och leverans av styrsystemet i enlighet med det avtal/kontrakt som bör finnas mellan köpare och säljare.

Arbetsgivarens straffrättsliga ansvar vid industriell verksamhet är mångfasetterat. Arbetsmiljölagen inklusive ellagstiftningen anger att arbetsgivaren har huvudansvaret för *arbetsmiljön*.

Arbetsmiljöns beskaffenhet regleras förutom av arbetsmiljölagen också av en mängd speciallagar, bl a ellagstiftningen. Det straffrättsliga ansvaret utkrävs alltid av en individ och bärs i allmänhet av företagets ledning, dvs VD eller styrelsen.

Grundläggande principer

Styrsystemet har en central roll i processen. Innan ett sådant projekteras är det därför viktigt att klargöra den överordnade filosofin för hur processen ska styras och övervakas och vilken säkerhetsnivå man kräver av systemet.

Grundläggande vid planering och projektering av styrsystem är detaljkunskap om den process som ska styras. Det är därför nödvändigt att experter inom både process- och styrsystem samarbetar när man arbetar fram ett nytt styrsystem. Lämpligen bildas en systemgrupp.

Handboken beskriver hur en sådan systemgrupp bör arbeta och vad som är grundläggande och viktigt att tänka på innan det detaljerade arbetet börjar.

Det grundläggande för planering av styrsystem är *processkunskap*. Processen och önskade styrfunktioner måste beskrivas i detalj som grund för det detaljerade projekteringsarbetet med styrsystemet. Om det inte är tillräckligt känt hur processen reagerar för den tänkta styrningen måste man först låta utföra en funktions- och säkerhetsanalys.

Den lönsamhet som styrsystemet förhoppningsvis bidrar till ska beakta alla de vinster och kostnader som är förknippade med styrsystemet under hela dess livslängd.

De faktorer som påverkar en anläggnings verkliga *prestationsförmåga* berörs, dvs teknisk prestation, driftssäkerhet och driftsmässighet.

Människa–maskinkommunikation. I ett operatörsbaserat styrsystem utgör *människan* den viktiga länken mellan styrsystem och process. Vad som bör beaktas i denna viktiga funktion beskrivs.

Handboken beskriver hur ett system kan byggas upp med *automation och övervakning, redundans och diversifiering*, dvs olika metoder av redundans.

Betydelsen av rätt organisation är grundläggande när ett styrsystem ska tas fram.

Såväl vid projekteringen som vid val av operatörer under drift är denna del mycket viktig att beakta och anpassa till styrsystemets storlek och komplexitet.

Genom att allt fler funktioner automatiseras finns risk för att operatören blir passivt övervakande i för hög grad då process och styrsystem fungerar väl.

Man kan minska dessa risker genom att göra operatörens övervakande uppgifter mer intressanta. Vidare är fortlöpande utbildning av operatörer angeläget i detta sammanhang.

Systemprestanda är viktiga att tänka på med avseende på bl a noggrannhetskrav, cykeltider, svarstider. Beträffande *samverkande system* ska säkerheten i kommunikationen mellan systemen beaktas.

Elektriska störningar berörs allmänt, samt dess olika störtyper, yttringar och normer.

Skilda typer av styrsystem beskrivs, t ex dedicerade-, programmerbara-, konventionella-, och blandade styrsystem, dvs *systemval samt tillvägagångssätt vid kvalificering av styrsystem*.

Grundläggande begrepp berörs om programvara, skilda modeller av programvara, programmeringsspråk, fel i programvara och programunderhåll.

Projektgenomförande

Säkerhetsansvaret för ett styrsystemprojekt måste fastställas före projektstart och samtidigt som projektorganisationen bildas.

Projektarbetets skilda aktiviteter gås igenom: beslutsetapper, kravspecifikationer, dokumentation och verifiering av styrsystem. Projektstrategi och kund–leverantörsförhållandet berörs också.

Vidare beskrivs skilda typer av *riskanalys* och kvalitetsäkringsmodell.

Förstudie/förprojektering

Det viktiga arbete som behöver göras för att få fram ett beslutsunderlag berörs.

Under rubriken *projektstrategi* behandlas vikten av att med ledning av resurser bestämma organisationsmodell och allmän uppläggning av projektarbetet.

Verksamhetsbeskrivning är det grundläggande underlaget för styrsystemets projektering i stort och i smått. Här berörs bl a vikten av styrfilosofi, processfunktioner och noggrannhetskrav.

Målet för styrsystemet måste klarläggas, dvs styrsystemets uppgifter. Här ska bedömas vilka funktioner som ska realiseras med hänsyn till processens möjlighet att ta emot styrning och vilka säkerhetsrisker som föreligger med de tänkta funktionerna.

Under rubriken *Drift och underhåll* beskrivs vikten av ett väl organiserat underhåll ur säkerhetssynpunkt.

Beslutsunderlaget är det material som projektet baseras på och som ger beslutsfattare tillräcklig information om det eventuella projektets lönsamhet, mål och syfte.

Projektering/upphandling

Projektorganisationen är viktig att fastlägga innan projektet startar. Beroende på det egna företagets resurser bestäms i vilken omfattning som extern hjälp i form av leverantörshjälp eller konsulter ska anlitas.

Projekteringsarbetet måste vara grundat på samarbete mellan specialister på skilda områden. Beroende på projektorganisationen kan dessa specialister bestå av egna eller externa resurser.

Styrsystembeskrivningen är det underlag som innehåller dels den grundläggande processbeskrivningen, dels den därpå framtagna övergripande funktionsbeskrivningen. På dessa basunderlag tas de mer detaljerade funktionsbeskrivningarna fram för projektering och senare konstruktion.

Kravspecifikationerna är det detaljerade underlag som ligger till grund för förfrågan och upphandling. Dessa ska utmynna ur en detaljerad projektering innan förfrågan utgår. Om en preliminär förfrågan utgår innan projekteringen är tillräckligt detaljerat utförd, är risken stor att anbudsunderlaget får arbetas om med extra kostnader som följd.

Upphandlingen är naturligtvis beroende på projektomfattning och därför av större eller mindre betydelse. Man bör dock i samtliga fall nogsamt beakta vilken detaljerad form av leverantörsåtaganden och kundåtaganden som ska ingå i upphandlingen. Åtminstone vid medelstora och större projekt ska ett kontrakt upprättas som innehåller såväl leverantörens som kundens detaljerade åtaganden i form av kravspecifikationer på såväl teknik som övriga åtaganden.

Konstruktion och tillverkning

Planering och konstruktion som behövs för *leverantörens* tillverkning behandlas allmänt.

Under rubriken *Kvalitetssäkring* berörs kvalitetssystemet SS–ISO 9001 som bygger på internationell standard och är liktydigt med svensk standard. Vidare behandlas projektmodellen för bl a konstruktion, sammansättning, kontroll, leverans/transport, montage, idrifttagning och dokumentation.

Systemkonstruktionen omfattar strukturering av leveransen, fysiskt och funktionellt. Hur systemet konfigureras med avseende på kravspecifikationer.

Detaljkonstruktionen beskriver vilket underlag som ligger till grund härför och hur kretskonstruktion och programkonstruktion går till.

Vidare behandlas människa–maskin-kommunikationen, bilduppbyggnad, rapport- och larmkonstruktion, maskinvarans sammansättning, elektriska störningar och skydd.

Säkerhetsanalysen beskriver den säkerhetskontroll som ska göras på den framtagna konstruktionen och vad som behöver kompletteras från säkerhetssynpunkt.

Tillverkning beskriver det på grundval av detaljkonstruktionen erforderliga arbetet för färdigställning av styrsystemet.

Leveranskontrollen behandlar den slutkontroll som måste till efter tillverkning och som kontrolleras dels hos leverantören, dels hos kunden, där kunden normalt deltar helt eller delvis.

Installation och montage

Det är angeläget att utrymmet planeras för såväl själva styrsystemet som för operatör, interface och elutrustning, dvs för all den teknikutrustning som ett styrsystem med funktioner innefattar.

Placering med hänsyn till underhåll, brandskydd, elstörning och klimat gås också igenom, liksom olika miljöklasser för hur kablar förläggs.

Elektriska störningar behandlas detaljerat.

Avstörningsregler, signalklasser och också jordning och skärmning vid ett stort antal kopplingsexempel finns åskådliggjorda med ritningar.

Minskning av elektrostatisk och magnetisk koppling genom separering och skärmning förklaras.

Systemmatning med olika metoder beskrivs, liksom jordning och skärmning.

Det är viktigt att montaget organiseras på rätt sätt ur ansvarssynpunkt. Detta beskrivs liksom allmänt utförande och montagekontroll.

Provning och idrifttagning

En beskrivning inleder av hur styrsystemet kontrolleras hos leverantörer enligt anvisningar, varefter mottagningskontroll sker hos köparen.

Det är viktigt att provning och idrifttagning sker välorganiserat ur säkerhets- och ansvarssynpunkt.

Skilda moment som åtgärder före spänningssättning liksom rörelse- och rotationsprov efter spänningssättning beskrivs.

Idrifttagning och verifiering beskrivs översiktligt.

Igångsättning av process

Såväl operatörer som drifts- och underhållspersonal måste ha för styrsystemet anpassad utbildning. Vad en sådan utbildning bör innehålla anges.

Före processtart ska viktiga försörjningar för styrsystemet kontrolleras enligt anvisning.

Driftsinstruktioner beskrivs liksom hur provdrift och åtgärdande av felaktigheter ska ske.

Kontraktsprov (verifiering) ska ske enligt anvisning efter en tids drift.

Överlämnande till driftsansvarig enhet ska ske med till systemet anpassad dokumentation. Leveransprov ska utföras tillsammans med driftsansvarig. Garantifrågornas hantering bestäms i enlighet med vad som har överenskommits i kontrakt.

Särskilda drifts- och underhållsrutiner ska föreligga enligt rekommendationerna.

Underhållsplanering och -anvisningar

I allt underhållsarbete är det grundläggande att klarlägga ansvarsfrågan avseende person- och saksäkerheten. Underhållstjänsten ska vara väl rustad för sin uppgift såväl organisatoriskt som med tekniska hjälpmedel. Tekniska felsökningshjälpmedel och fullständig dokumentation över anläggningen och dess funktioner är mycket viktigt för en väl fungerande underhållstjänst.

Snabb tillgång till reservdelar är viktigt.

Det är likaså viktigt att underhållsorganisationen är anpassad till anläggningens tekniska nivå. Därför ska underhållspersonalen ha kompetens i förhållande till den tekniska utrustningen.

Tekniska hjälpmedel rekommenderas för bl a felsökning och reservdelslager.

Utbildning och dokumentation

Avslutningsvis redogör handboken för grundläggande och fortlöpande behov av utbildning för skilda typer av personal som på något sätt arbetar med eller har ansvar för styrsystem. Här redovisas också krav på den dokumentation som ska finnas väl tillgänglig och rätt uppdaterad för anläggningen i fråga.

RAPPORTEN

FIE-SAFE, Handbok. Programmerbara Elektroniska Styrsystem. Säkerhet inom industrin. Rekommendationer och anvisningar (334 sidor) kan beställas från FIEs kansli, Box 8133, 104 20 Stockholm, tel 08-657 12 06, fax 08-653 20 77. Pris: 900 kronor för medlemmar i FIE, 1 900 kronor för icke medlemmar.

Föreningen för Industriell Elteknik, FIE

FIE är en ideell förening som bildades 1960. Medlemmar är företag och personer inom process- och verkstadsindustrin samt leverantörer, entreprenörer och konsulter verksamma inom industrin. FIE har cirka 200 företagsmedlemmar, och cirka 400 personliga medlemmar, t ex elchefer, underhållschefer och elingenjörer.

ORD&FORM AB, Uppsala 1994 Best.nr. 626-1933-0

Sammanfattning 1662 Januari 1994
Pnr 87-0922 Olycksfall, tekniska åtgärder (46)

Arbetsmiljöfonden

Postadress **Box 1122, 111 81 Stockholm** ***Besöksadress*** **Olof Palmes Gata 31** ***Tel*** **08-791 03 00** ***Fax*** **08-791 85 90**