Prover Technology AB

Formell verifiering av CST ställverk

Metodik I - Introduktion

Per Larsson, Ilya Beylin och Karin Helander

29 januari 2010

Pi-CST-LFD-1
Utgåva: 1.0
Sidor: 20

PROVER™
TECHNOLOGY

Innehåll

Figurer

Tabeller

1 Inledning

Företaget Prover Technology AB (fortsättningsvis *Prover*) har under de senaste åren varit involverad i en rad projekt som gällt automatiserad granskning av ställverkssystem i Stockholmsområdet, s.k. friförbundna ställverk av typen CST. Företagets speciella kompetens är att analysera komplexa system med *formella metoder*. Mycket förenklat innebär metodiken att först beskriva systemet och säkerhetskraven i ett logiskt språk, i nästa steg är det möjligt att använda datorstöd för att säkerställa att säkerhetskraven är uppfyllda. Syftet med detta dokument är att ge en övergripande introduktion till metodiken och hur den har applicerats i CST området. En mer tekniskt detaljerad beskrivning av denna process ges i fördjupningsdelen av detta dokument i [11].

2 Arbetsprocess

Användandet av formella metoder kan generellt delas in i fyra delmoment:

(i) Först måste det fastslås vilken del av och vilka egenskaper hos det verkliga systemet som skall beskrivas.

(ii) När avgränsningen är gjord så beskrivs, *modelleras*, de utvalda egenskaperna av systemet i ett logiskt språk, resultatet utgör en *systemmodell*.

(iii) I nästa moment så formuleras också kraven som ska ställas på systemet i samma logiska språk, resultatet utgör en *kravmodell*.

(iv) I det sista momentet, *analysfasen*, försöker man bevisa att de beskrivna kraven är uppfyllda för systemet.

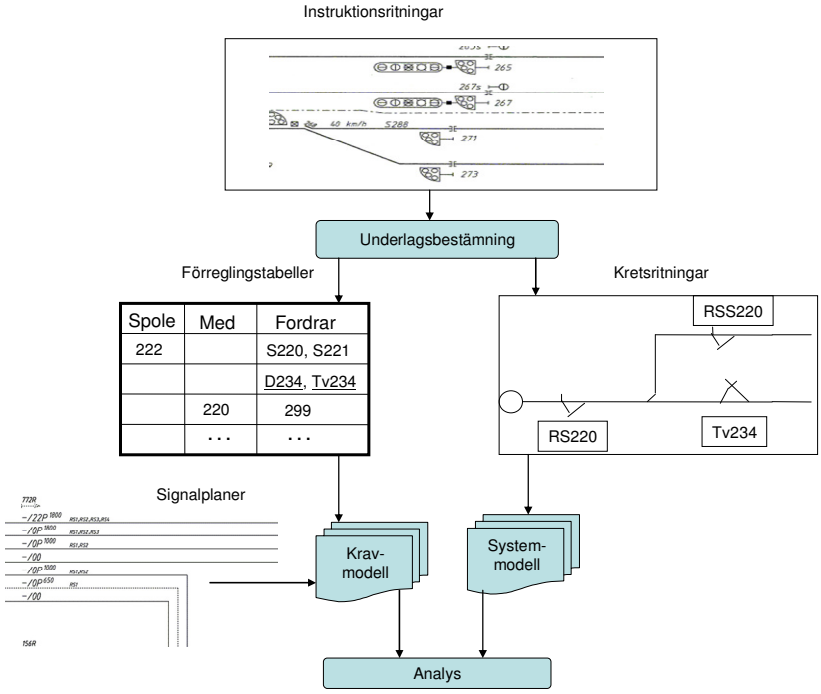
Fortsättningsvis ska vi ibland något slarvigt tala om ”systemet” och låta sammanhanget avgöra det är det verkliga systemet eller den logiska beskrivningen, d.v.s. systemmodellen, som avses. I analysfasen vill man visa att kraven är uppfyllda i alla möjliga tillstånd som systemet kan befinna sig i. Detta utgör också den stora attraktionen med formella metoder, med traditionella metoder som testning och simulering kan man endast kontrollera en bråkdel av alla tillstånd i ett större system. Den formella analysen utförs oftast med hjälp av speciell programvara, med datorstöd är det möjligt att analysera krav gentemot en systemmodell som kan innehålla tusentals variabler. Vid utförda analyser av CST ställverk har de fyra delmomenten ovan bedrivits på följande sätt:

(i) I samråd med uppdragsgivaren avgränsas först vilket geografiskt delområde som ska analyseras. Mer precist väljer man ut de bangårdsobjekt, signaler, växlar och spårledningar, som ska ingå i verifieringen. Ett viktigt hjälpmedel vid avgränsningen är den s.k. instruktionsritningen för projekteringsområdet. I detta skede bestäms också vilka funktionella egenskaper i systemet som ska analyseras, exempelvis har inte manöversystemet för det utvalda området analyserats i tidigare projekt . I avsnitt 5 beskrivs mer utförligt hur systemet avgränsas.

(ii) Den geografiska och funktionella avgränsningen bestämmer i sin tur vilka reläer i ställverket som ska ingå i analysen. De relevanta kretsritningarna för dessa reläer utgör det huvudsakliga underlaget för systemmodellen. Systemmodellen utgör en beskrivning av strömsättningsvillkoren för reläspolarna. Modelleringen av systemet beskrivs i avsnitt 6.

(iii) De krav på ställverket som modellerats är dels *säkerhetskrav*, egenskaper som måste vara uppfyllda för att förhindra olyckor, dels *funktionella krav,* som ska vara uppfyllda för att undvika onödiga driftsstopp. Indata för kravmodellen utgörs av förreglingstabeller, upplåsningstabeller, signaleringsplaner samt dokument som specificerar generiska krav för CST ställverk. Modellering av krav beskrivs i avsnitt 8. Det logiska språk som använts i system- och kravmodell är s.k. *temporallogik* som beskrivs i avsnitt 3.

(iv) I analysfasen kontrolleras att alla säkerhetskrav och funktionella krav är uppfyllda med datoriserade metoder, se avsnitt 9. Verifieringsverktyget som används är Prover iLock Verifier som beskrivs i avsnitt 4.



Figur 1 Process – CST verifiering

I figuren ovan visas en översiktbild av arbetsprocessen. I de följande avsnitten av detta dokument ges mer detaljerade beskrivningar av hur de olika arbetsmomenten utförs.

3 Modelleringsspråk

Logiska beroenden mellan reläer och dess kontakter i ställverk är i vissa fall sekventiella, d.v.s. för att kunna beskriva värdet för ett relä måste man ha tillgång till en och ibland flera föregående värden för andra reläer. För att kunna representera sådana temporala beroenden används s.k. *temporallogik*. Nedan ges en kortfattad och informell beskrivning av det temporallogiska språk som använts i projekten.

Inledningsvis ges en beskrivning av alla formler i språket med hjälp av följande definition:

(i) En variabel är en formel.

(ii) Konstanterna *TRUE* och *FALSE* är formler.

(iii) Om *a* och *b* är formler så är också *a* & *b*, *a* # *b*, *a* → *b* och ~*a* formler.

(iv) Om *a* är en formel så är också *X(a)* och *I(a)* formler.

Logiska variabler, beskrivna i den första klausulen, används i systemmodellen för att representera ställverkskomponenter som reläspolar, reläkontakter, dioder och kondensatorer etc. Dessa variabler kan endast ha ett av två olika värden, sann eller falsk. När variablerna som i detta sammanhang representerar komponenter i ett kretssystem är det naturligt att tolka dessa två värden som att en given komponent är strömförande eller inte. Beteckningarna *1* och *0* används också fortsättningsvis ibland för dessa två sanningsvärden.

Konstanterna TRUE och FALSE, i den andra klausulen, representerar en alltid sann respektive en alltid falsk formel.

Formlerna i den tredje klausulen uttrycker sammansatta villkor och har följande informella tolkningar:

a & *b*, konjunktion, ”*a* och *b*”

a # *b*, disjunktion, ”*a* eller *b*”

a → *b*, implikation, ”om *a* så *b*”

~*a,* negation, ”inte *a*”

Logisk disjunktion, *a* # *b*, ska tolkas inklusivt, d.v.s. formeln är sann när någon eller båda av alternativen är sanna. Logisk implikation, *a* -> *b*, är endast en bekväm förkortning för formeln ~*a* # *b*.

Formlerna i den fjärde klausulen används för att uttrycka tidsegenskaper och har följande informella tolkningar:

I(*a*), ”initialt *a*” eller ”i starttillståndet gäller *a*”

X(*a*), ”i nästa tidssteg gäller *a*”.

De logiska formlerna används i *definitioner* för att beskriva beteendet för komponenter i systemmodellen. Med hjälp av parvisa definitioner på formen

I(*v*) := *initialtillstånd*

X(*v*) := *villkor*

beskrivs det möjliga beteendet för en variabel *v* i alla tidssteg. Den första formen används för att beskriva starttillståndet för *v* och den senare för att beskriva beteendet för *v* i alla efterföljande tidssteg. Se exempelvis de två definitionerna

```
I(D364_S) := FALSE;
X(D364_S) := S364_F & S364/bdisp_F & H364_F;
```

(Suffixen ”_S” och ”_F” betecknar här spolar respektive frontkontakter av ett relä, se avsnitt 6.1). Den informella tolkningen av dessa definitioner är:

> ”spolen D364_S är initialt fallen”;
>
> ”spolen D364_S är dragen i nästa tidssteg om (och endast om) alla kontakterna i högerledet är slutna i nuvarande tidssteg”.

Dessa definitioner utgör också ett exempel på ett typiskt användande av logiska definitioner i systemmodellen. Beteendet för en reläspole beskrivs genom att specificera dess initiala tillstånd och dess möjliga tillståndsförändringar.

Den exakta tolkningen av temporala formler ges relativt en s.k. *modell* som tilldelar, för varje tidssteg, ett sanningsvärde till varje variabel. Givet en sådan modell kan man sen avgöra värdet för alla sammansatta formler. Exempelvis så är formeln *a* & *b* sann i tidssteget *t* om både *a* och *b* är sanna i detta tidssteg och formeln X(*a*) är sann i tidssteget *t* om *a* är sann i tidssteget *t+1*. Notera att begreppet *tidssteg* avser en abstrakt enhet som representerar en tillståndsövergång i systemet. Det är alltså inte möjligt att i detta språk uttrycka systemegenskaper som rör tid i form av verkliga tidsenheter som exempelvis sekunder.

4 Verktygsstöd

Vid modelleringsfasen används ett flertal verktyg. Detta är nödvändigt för att kunna effektivisera processen att översätta den stora datamängden i kretsritningar, förreglingstabeller, m.m., till ett logiskt format. Det viktigaste hjälpmedlet i denna fas är Prover iLock Extractor som används för att extrahera information om reläer och reläförbindelser i CAD-ritningar. Mer information om detta verktyg finns i produktspecifikationen [2] och i tillämpningsbeskrivningarna [2].

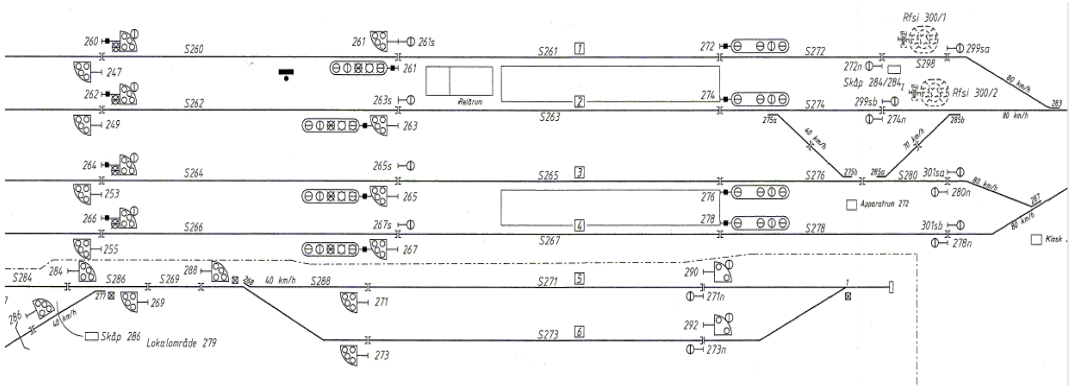
Vid analysfasen används verktyget Prover iLock Verifier, som är en logisk bevismotor. Mer information om verktyget ges i rapporten [4]. Givet en inmatad systemmodell och kravmodell kan verktyget avgöra om kraven är uppfyllda. Om ett speciellt krav inte är uppfyllt producerar verktyget en så kallad *motmodell* som innehåller detaljerad information om orsakerna till att kravet inte är giltigt, sådana motmodeller beskrivs närmare i avsnitt 9.1.

5 Avgränsning av system

För att definiera det system som ska analyseras görs avgränsningar enligt förfrågningsunderlaget. Man kan tala om två olika typer av avgränsningar. Dels avgränsningar av geografisk art, d.v.s. vilket område och komponenter som ingår i systemet, men också funktionella avgränsningar som avser vilka egenskaper i det verkliga systemet som ska representeras i systemmodellen.

5.1 Geografiska avgränsningar

Systemets utsträckning, definierade i förutsättningarna för projektet, bestämts av vilka signaler, växlar och tågvägar som ska ingå i analysen, vilket i sin tur bestämmer vilka reläer som ingår i systemmodellen. För att få överblick över vilken del av ställverket som ska modelleras utgår man från den så kallade *instruktionsritningen*, som är en översiktlig presentation av bangården med dess signaler och växlar. I figuren nedan visas ett mindre avsnitt av en sådan ritning.



Figur 2 Instruktionsritning

5.2 Funktionella avgränsningar

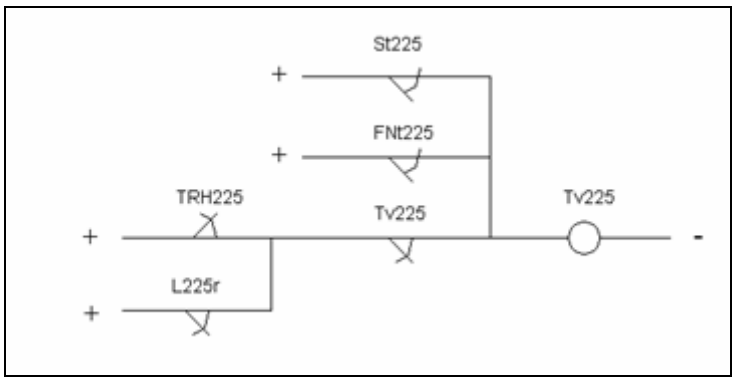
Ett exempel på funktionella avgränsningar som gjorts, i samråd med uppdragsgivaren, vid tidigare verifieringsprojekt gäller modelleringen av manöversystemet. Reläer som interagerar med manöversystemet har visserligen ingått i systemmodellen men har tilldelats konstanta värden, d.v.s. de antas vara låsta i ett fixt läge. Detta innebär att systemkraven kontrollerats utifrån antagandet att de manuellt styrda reläerna aldrig slås om ifrån sina initiala lägen.

6 Systemmodell

I detta avsnitt beskrivs översiktligt hur systemmodellen skapas utifrån indata i form av kretsritningar för reläsystemet.

6.1 Kretsritningar och modellering av reläer

Kretsritningarna är det huvudsakliga underlaget för systemmodellen. Ritningarna representerar utformningen av ett reläsystem som, utifrån indata från spårledningar, tågvägar, växellägen m.m., sedan styr centrala funktioner som exempelvis: växelomläggningar, förregling av rörelsevägar och signalering. Varje kretsritning beskriver beteendet för en eller flera reläspolar. Ett relä består av en spole, som styr värdet för ett antal kontaktpunkter, benämna front- och backkontakter.



Figur 3 Kretsritning

I figuren ovan (Figur 3) visas en förenklad kretsritning (data som rör ram, stativ- och kontaktnummer m.m. är utelämnat). Kretsen visar beteendet för spole Tv225. Symbolerna ”+” och ”–” betecknar plusnoder respektive minusnoder, de övriga symbolerna har följande tolkning:

	Icke remanent reläspole, om reläet har namnet X så betecknas dess spole med namnet X_S.
	Frontkontakt till reläspole, om reläet har namnet X så betecknas frontkontakten med namnet X_F
	Backkontakt till reläspole, om reläet har namnet X så betecknas backkontakten med namnet X_B.

Linjerna i kretsritningen visar hur komponenterna är förbundna. En väg från en plusnod via en spole som sedan avslutas i en minusnod är en möjlig strömsättningsväg för spolen i kretsen. Med utgångspunkt från exemplet ovan visas nedan hur modelleringen av reläspolar utförs. Den logiska översättningen av kretsen ovan i figuren systemmodellen ges av följande definition:

```
X(Tv225_S) :=
    St225_F # FNt225_F # (Tv225_F & (TRH225_B # L225r_F));
```

Definitionen ovan utläses : ”Tv225_S är dragen i nästa tidssteg om det nu gäller att antingen St225_F är sluten eller att FNt225_F är sluten, eller …”. Definitionen beskriver alltså alla möjliga sätt för hur spolen Tv222_S kan strömsättas. Definitionen ovan kompletteras sedan med en beskrivning av initialtillståndet för spolen som ges av dess s.k. *normaltillstånd*, i detta fallet:

```
I(Tv225_S) := TRUE;
```

Detta par av definitioner utgör en beskrivning av spolens beteende i alla tidssteg. Det kvarstår endast att specificera det logiska beroendet mellan reläspolen och dess kontakter. I detta fall, för ett s.k. icke remanent relä, är relationen trivial och ges av definitionerna nedan:

```
Tv225_B := ~Tv225_S;
Tv225_F := Tv225_S;
```

Dessa definitioner uttrycker att frontkontaktens variabel är sann endast när spolen är strömförande och att backkontakten är sann endast när spolen inte är strömförande.

De flesta relänamn i CST-ställverk är knutna till en viss funktion. Exempelvis är ett relä med namnet L222 knuten till låsning och upplåsning av tågvägar med början i signal 222. Fortsättningsvis används i detta dokument beteckningar på formen L###, *A*###, o.s.v. där strängen ### avser ett godtyckligt objektnamn för en växel eller signal (oftast ett tresiffrigt nummer).

6.2 Förbindelselistor

Eftersom verifieringsprojekt kan omfatta innehållet i hundratals kretsritningar skulle det bli mycket tidskrävande att manuellt översätta ritningarna till logiska uttryck. I syfte att effektivisera denna process används ett komprimerat textuellt format, s.k. *förbindelselistor*, som representerar reläer och reläförbindelser i kretsritningen. Varje rad i förbindelselistan innehåller data om två förbundna komponenter i kretsritningen. Från förbindelselistan är det sen möjligt att automatiskt generera den logiska översättningen. I figuren nedan visas ett utdrag från en förbindelselista som representerar en krets i S110 området

Ta bort rad vid markering				A-ända							Infoga rad under markering	B-ända					
Rad	Ver	Förändr	Area	Undernr	Blad	Komp	Beteckning	Index	Klämma	Stativ	Undernr.	Blad.	Komp.	Beteckning.	Index.	Klämma	Stativ.
1	Ä0325			252	2	m	m				252	2	re	J151		54	79
2	Ä0325			252	2	re	J151		52	79	252	2	re	J165		16	92
3	Ä0325			252	2	re	J165		15	92	252	2	p	p			
4	Ä0325			252	2	m	m				252	2	Fd	Fd1/79		16	
5	Ä0325			252	2	Fd	Fd1/79		15		252	2	re	J151		51	79
6	Ä0325			252	2	re	J151		53	79	252	2	re	J151		54	79
7	Ä0325			252	2	re	J151		51	79	252	2	Td	Td1/79		16	
8	Ä0325			252	2	Td	Td1/79		13		252	2	re	J151		11	79
9	Ä0325			252	2	Fd	Fd1/79		14		252	2	Td	Td1/79		15	
10	Ä0325			252	2	Td	Td1/79		14		252	2	m	m			
11	Ä0325			252	2	Td	Td1/79		15		252	2	re	J151		12	79
12	Ä0325			252	2	re	J151		11	79	252	2	re	RSS756+	I	17	97
13	Ä0325			252	2	re	RSS756+	I	18	97	252	2	re	RS165		202	92
14	Ä0325			252	2	re	RSS756+	I	17	97	252	2	re	RS165		201	92
15	Ä0325			252	2	re	FNt165		14	91	252	2	re	RS151		12	80
16	Ä0325			252	2	re	FNt165		13	91	252	2	re	RS160B		5	85
17	Ä0325			252	2	re	RS151		12	80	252	2	Td	Td1/79		16	
18	Ä0325			252	2	re	RS151		11	80	252	2	re	RS160B		6	85
19	Ä0325			252	2	re	RS160B		5	85	252	2	re	RS160		14	85
20	Ä0325			252	2	re	RS160		13	85	252	2	re	RS165		202	92
21	Ä0325			252	2	re	RS165		201	92	252	2	re	J165		18	92
22	Ä0325			252	2	re	J165		17	92	252	2	p	p			

Figur 4 Förbindelselista

Förbindelselistan utgör ett flexibelt mellanformat, mellan kretsritningen och systemmodellen, som är oberoende av vilket designverktyg som användes för att skapa den ursprungliga ritningen. För nyare ritningar är det också möjligt, med hjälp av verktyget Prover iLock Extractor, att automatiskt producera en förbindelselista givet en CAD-ritning i DGN-format. För äldre CAD-ritningar och tuschade ritningar, måste emellertid översättningen till förbindelselistan ske med delvis manuella metoder. En värdefull egenskap med förbindelselistan är att den kan användas som underlag för en rad tidsbesparande kontroller i projekteringsarbetet. Mer detaljer om tillämpningar som utnyttjar förbindelselistor finns beskrivna i rapporten [2].

6.3 Modellering av hårdvarufel

I den normala modellen av ställverket antas att komponenterna fungerar felfritt. I en alternativ systemmodell, en s.k. *felmodsmodell*, simuleras möjligheten att ställverkskomponenter kan sluta fungera. Det är inte möjligt att modellera alla typer av feltillstånd som, åtminstone i teorin, skulle kunna uppstå i ställverket. Hur stabilt ett industriellt system än är utformat kan det svårligen uppfylla alla säkerhets- och tillgänglighetskrav i en situation där, låt oss säga, samtliga hårdvarukomponenter samtidigt går sönder. Analys av hårdvarufel, oavsett om den är formell eller argumenterande, kompletteras därför vanligen med en riskanalys, där man bedömer sannolikheten och allvaret för olika typer av hårdvarufel. I detta fall har uppdragsgivaren gjort denna analys och bestämt urvalet för vilka typer av fel som ska ingå i felmodsmodellen.

Inledningsvis analyseras endast fel för reläer men ej för andra typer av ställverkskomponenter såsom transistorer och dioder. Man skiljer mellan två olika huvudtyper av reläfel. Dels att en reläspole inte kan bli strömförande, vilket leder till att dess frontkontakter fortsättningsvis alltid är slutna och att dess backkontakter fortsättningsvis alltid är öppna. Detta fel kan exempelvis uppstå genom avbrott i ledningen fram till spolen eller avbrott i själva reläet. Sådana fel är inte helt ovanliga och ställverket ska utformas så att säkerheten i systemet bibehålls även om de inträffar. Den andra huvudtypen av reläfel är s.k. ”klibbning” där en kontakt fastnar i ett fixt läge oberoende av spolens värde. Detta fel bedöms vara riskabelt, men också mer sällsynt i praktiken. Felmodsmodellen inkluderar inte denna senare typ av fel

Ytterligare en aspekt av ett systems stabilitet vid förekomster av hårdvarufel gäller antalet samtidiga fel som systemet säkert kan hantera. Ett s.k. *enkelfel* innebär att endast ett relä felar, ett *dubbelfel* innebär att två reläer felar samtidigt, o.s.v. I den formella felmodsmodellen undersöks endast enkelfel. I avsnitt 9.2 beskrivs mera om hur reläfel behandlas i analysfasen.

7 Systemmodell, begränsningar

Det enkla logiska språk som används i systemmodellen kan inte fullständigt beskriva alla komplexa händelser och egenskaper i det verkliga systemet. Vissa verkliga egenskaper utelämnas helt i modellen, andra egenskaper beskrivs endast ungefärligt. I avsnittet 6.3 ovan visades exempelvis hur endast en delmängd av alla möjliga feltillstånd i ställverket blir representerade i modellen. Till skillnad från bevisning av krav, som är en formell relation mellan modell och krav, måste man i detta fall ge informella argument för att modellen faktiskt är en godtagbar representation av det verkliga systemet. I detta avsnitt diskuteras några systemegenskaper som är speciellt svåra att uttrycka i modellen.

7.1 Synkron modellering av asynkrona system

Ett elektriskt reläställverk är ett exempel på ett *asynkront* system, d.v.s. händelser i systemet i form av tillståndsövergångar för komponenter, kan inträffa vid vilken tidpunkt som helst. I flertalet datoriserade ställverkssystem är däremot tillståndsövergångarna styrda av en synkroniserande systemklocka. Den logiska modellen har större likheter med ett sådant synkront system, där alla tillståndsövergångar dessutom antas genomföras samtidigt och omedelbart. Denna representation är godtagbar om man antar att det verkliga ställverket reagerar ”tillräckligt fort” på tillståndsförändringar. Om säkerhetskritiska fel kan uppkomma i det verkliga ställverket pga. exempelvis kapplöpningseffekter mellan olika händelser så kan detta inte upptäckas i systemmodellen.

7.2 Tidsegenskaper

Det är inte möjligt, i det valda logiska språket, att uttrycka egenskaper som rör exakta tidsintervall. Sådana intervall återfinns emellertid i det verkliga systemet i form av tidsfördröjande komponenter såsom kondensatorer och tiddon. I systemmodellen approximeras sådana egenskaper istället med fördröjningar av ett godtyckligt antal abstrakta tidssteg. Detta är ett exempel på hur man i modellen ibland tillåter logiska scenarier som faktiskt aldrig kan uppkomma i det verkliga systemet. Sådana försvagningar av modellen kan inte leda till att eventuella verkliga fel förblir oupptäckta under analysen, däremot finns möjligheten att egentligt uppfyllda systemkrav inte kan bevisas i modellen just pga. av att man tillåtit orealistiska tillstånd i modellen.

7.3 Yttre händelser

Ställverket har ett gränssnitt till detektorer som avläser yttre händelser i bangården som exempelvis spårbeläggning och växellägen. Det finns speciella reläer i systemet som sedan mottar dessa händelser. I systemmodellen representeras huvudsakligen sådana spolar med odefinierade, *fria variabler,* vilket innebär att de kan anta ett godtyckligt värde i varje tidssteg i modellen. Exempelvis representeras spårledningsreläer i ställverket med fria variabler. Ofta finns emellertid naturliga begränsningar för hur de yttre händelserna kan påverka det reella ställverket. Exempelvis så kan i verkligheten inte en spole som detekterar läget för en växel ändra sig godtyckligt snabbt då själva omläggningen inte kan vara omedelbar. Även dessa typer av begränsningar kan endast ges en ungefärlig representation i systemmodellen.

8 Kravmodell

I detta avsnitt beskrivs översiktligt hur kravmodellen skapas utifrån indata i form av förreglingstabeller, signaleringsritningar och beskrivningar av generiska krav.

8.1 Förreglingstabeller, låsningskrav och upplåsningskrav

De s.k. förreglingstabellerna innehåller logiska krav för reläerna uttryckta på en relativt låg nivå. Förreglingstabellerna är ett viktigt underlag i projekteringsarbetet i Stockholmsområdet då de används som en funktionell specifikation av designen för kretsritningarna. Under de senaste åren har det precisa formatet för dessa tabeller genomgått ett flertal olika förändringar. I dokumentet [5] ges en beskrivning av det senaste formatet för tabellerna som ska användas vid nya projekteringar. Det schematiska innehållet tabellerna är dock likartat i de olika formaten. För kritiska reläer som i första hand kontrollerar låsning och upplåsning av tågvägar specificeras vilka villkor som ska vara uppfyllda när reläspolen är strömförande. I bilden nedan visas ett kort utdrag från en äldre förreglingstabell för Tegelbacken, spår 17-19.

Låsrelä	**Med**	**Fordrar**	**Om ej**
418		D418, Tv418	
418		D406, Tv406	
418		575r	
418		587r	573
…	…	…	…

Tabell 1 Utdrag från förreglingstabell

Just detta tabellformat har följande informella tolkning: I den första kolumnen anges vilken reläspole som beskrivs, i detta fall backspolen för det remanenta reläet L418. I kolumnen *Fordrar* anges vilka villkor som ska vara uppfyllda om spolen är strömförande. Kolumnerna *Med* och *Om ej* anger eventuella sidovillkor som också ska vara uppfyllda för att raden ska vara relevant. Namnen i kolumnerna *Med*, *Fordrar* och *Om ej* syftar på reläkontakter, om namnet inte är understruket så är det kontakten som är aktiverad i normalläget, annars den motsatta kontakten. Om flera namn förekommer i villkorskolumnerna tolkas detta som att alla angivna kontakter ska vara slutna. Den schematiska översättningen av en rad i tabellen är:

```
Relä & Med & ~Om_ej -> Fordrar
```

Varje rad anger ett nytt villkor för reläet. Givet extra information om normalläget för ingående reläer i villkorskolumnerna och om vilken spole som tabellerna gäller får vi detta första förenklade försök till en logisk översättning av exemplet:

```
(X(L418_SB) -> (D418_F & Tv418_B))    &
(X(L418_SB) -> (D406_F & Tv418_B))    &
(X(L418_SB) -> 575r_F)                &
(X(L418_SB) & ~SS573+_F -> L587r_F)   &
...
```

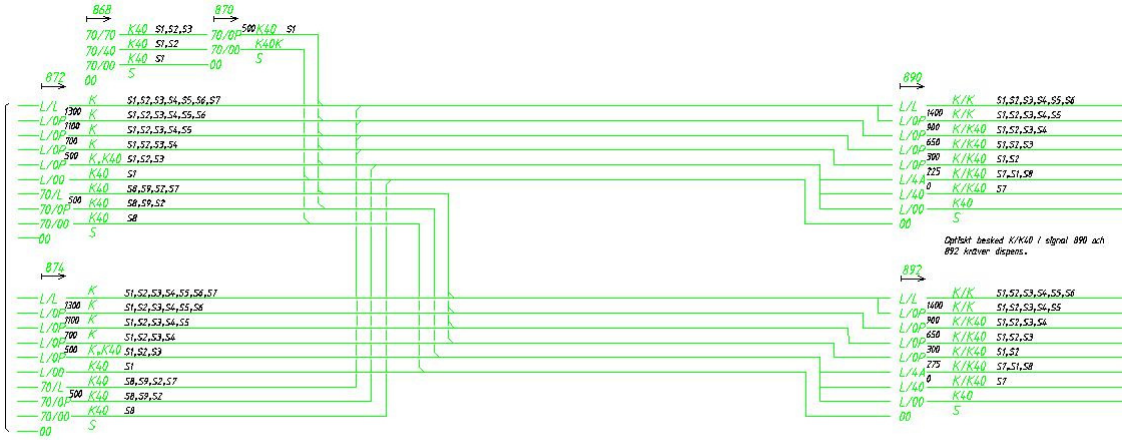
Metodiken för att modellera upplåsningskrav är likartad. Tyvärr saknas en del nödvändig information i förreglingstabellerna. Kraven gäller inledningsvis endast under förutsättning att vissa manöverreläer och kondensatorer i kretsen inte är aktiverade. Vidare finns det också dolda förutsättningar angående när kraven i tabellerna ska vara uppfyllda: För vissa reläer antas kraven endast gälla vid reläomslag, för andra reläer

gäller kraven endast efter en viss tidsfördröjning, o.s.v. För att göra den slutliga översättningen krävs därför mer kunskaper om den precisa tolkningen av kraven för olika typer av reläer.

8.2 Signaleringsplaner och signaleringskrav

Verifieringen omfattar också krav på reläer som berör signaleringen. Indata för att skapa dessa krav är instruktionsritningen och signaleringsplanerna för projekteringsområdet. Nedan ges endast en översiktlig beskrivning av dessa krav, mer information ges i fördjupningsdelen [11]. Banverkets egen beskrivning av vilka signaleringskrav som ska kontrolleras ges bl.a. i dokumenten [9] och [10].

Signaleringsplanen visar områdets signaler med information om dess olika signaleringsbilder, ATC-besked, kombinationer av styrsignalreläer (###S*N*) samt beroenden mellan signalbilder i olika signaler. I figuren nedan visas ett utdrag från en signaleringsplan för Sundbyberg.

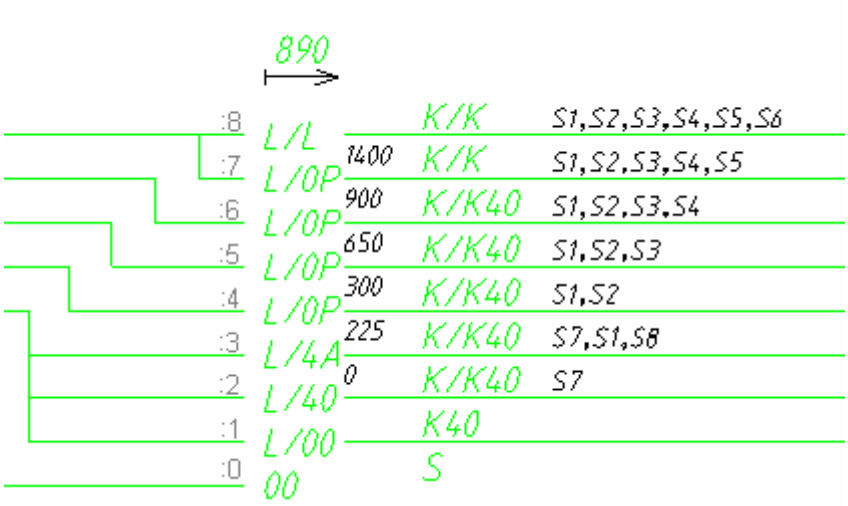


Figur 5 Signaleringsplan

Till skillnad från fallet med kretsritningarna så finns det för närvarande inte någon helt tillfredställande mekanisk metod för att utvinna den grafiska informationen i signaleringsplanerna till ett textuellt format. Detta får därför göras med manuella metoder.

Varje signalbild i signalplanen motsvaras i ställverket av en logisk kombination av signalreläer (A-, B-, C-, Gul- och Förs- reläer). Denna information är inte utskriven direkt i signaleringsplanerna men är likartad för alla CST-områden. Exempelvis motsvaras ”K/K” (Kör vänta Kör) av A- och Förs- reläer för signalen medan ”K” motsvaras av endast A-reläet, o.s.v.

Vissa av kraven för signalreläerna och styrsignalreläer formuleras utifrån en *startsignal* och dess *målsignaler*, där en målsignal är en omedelbar grannsignal i körriktningen. Extra information om vilka växellägen som krävs för att köra från en startsignal till en given målsignal måste hämtas från instruktionsritningen. I exemplet ovan krävs bl.a. växelläge 881+ för vägen från signal 872 till 890. För att resonera om kraven underlättas också om de olika signaleringsnivåerna för en signal tänks vara numrerade från 0 i stoppbeskedet och uppåt (se förstorad bild i Figur 6 nedan).



Figur 6 Signaleringsplan för signal 890, med tillskrivna nivåer 0 – 8

Krav för ATC styrsignalreläer

Givet en startsignal ### kontrolleras sammanfattningsvis följande egenskaper för samtliga styrsignalreläer för signalen (reläer på formen ###S*N*).

1. Kontroll av ljusrelä för grönt sken (Ljg###_F)
2. Kontroll av signalreläerna (A###_F, B###_F eller C###_F) i den mån respektive relä finns i ställverket
3. Kontroll av målsignalernas nivåer

Den sista punkten kräver en mer utförlig förklaring. Vi använder oss av figuren ovan och exemplifierar kraven för reläet 872S4. Detta relä är enligt signaleringsplanen aktiverat i signaleringsnivåerna 6-9 för signal 872. Dessa nivåer är i sin tur förbundna till nivåerna 4-8 i målsignalen 890. Kontrollen av de avsedda målnivåerna görs genom att kontrollera växelläge (881+ i detta fall) och de listade styrsignalreläerna i respektive målnivå. För exemplet förutsätts att endast A- och B-relä finns för signal 872 samt att det finns hjälpdefinitioner för de listade styrsignalreläerna för de aktuella målnivåerna på formen:

```
890:4 := 890S1_F & 890S2_F;
890:5 := 890S1_F & 890S2_F & 890S3_F;
…
```

Givet dessa förutsättningar görs följande logiska formulering av kraven 1-3 ovan för 872S4:

```
1) X(872S4_S) -> Ljg872_F;
2) X(872S4_S) -> A872_F # B872_F;
3) X(872S4_S) -> SS881+_F &
   ( 890:4 # 890:5 # 890:6 # 890:7 # 890:8 );
```

Den beskrivna mekaniska genereringen av kraven ovan resulterar emellertid i vissa fall i alltför starka kravformuleringar. Dessa och andra komplikationer i samband med signaleringskraven beskrivs i fördjupningsdelen [11] samt i Banverkets dokument [9].

Krav för optisk signalering

Givet en startsignal ### kontrolleras sammanfattningsvis följande egenskaper för samtliga reläer för optisk signalering i signalen (reläer på formen A###, B###, C###, Gul### och Förs###)

1. Kontroll av låst tågväg (L###_B) samt gemensamma krav för signalen.
2. Kontroll av s.k. nedtrappningsspärr (StA###_F respektive StA/B###_F)
3. Kontroll av målsignalernas signaleringsnivåer

De ”gemensamma kraven” nämnda i punkt 1 finns specificerade i förreglingstabellen. Kontrollen i punkt 2 ovan syftar till att förhindra att man inte kan skifta från ett högre till ett lägre optiskt körbesked i huvudljussignal, se vidare beskrivning i [10]. Punkt 3 är liknande kontrollen av målnivåerna i fallet med styrsignalreläerna ovan, men här istället formulerad i form av kombinationer av signalreläer för de avsedda målnivåerna.

8.3 Generiska krav

Utöver de krav som finns dokumenterade i förreglingstabeller eller skapas utifrån signaleringsplanerna finns en mängd *generiska krav* för reläerna. Med detta menas krav som förväntas vara uppfyllda för alla reläer av en viss typ, vid alla CST ställverk. Underlaget för vilka generiska krav som ska kontrolleras har getts av Banverket i dokumentet [10]. Nedan visas ett utdrag från en tabell som visar några av de generiska krav som analyserats i tidigare projekt.

Spole	**Krav**
A###_S	L###_B, St###_B
B###_S	L###_B, St###_B
…	…

Tabell 2 Utdrag från generiska krav

Något förenklat så skapas sedan från tabellen, och matchande reläer i ett projekteringsområde, krav med utseendet:

```
X(A222_S) -> L222_B & St222_B;
X(A224_S) -> L224_B & St224_B;
…
```

Den slutliga översättningen av de generiska kraven kompliceras dock, analogt med fallet för upplåsnings- och låsningskrav, av implicita förutsättningar om de berörda reläkretsarna.

8.4 Strömsättningskrav

En grundläggande förutsättningen om systemet är att samtliga reläspolar i något tillstånd kan vara dragna och i något tillstånd kan vara fallna. Denna typ av grundläggande funktionskrav för spolarna benämns fortsättningsvis *strömsättningskrav*. Mer exakt så innebär detta att man för varje relä kontrollerar att

- spolen kan vara dragen;
- spolen kan vara fallen;
- spolen kan slå om från fallen till dragen;
- spolen kan slå om från dragen till fallen;

9 Analys av krav

När modelleringen av systemet och kraven är klar är det möjligt att starta själva analysarbetet. I princip skulle man nu kunna låta bevismotorn arbeta klart med systemmodell och kravmodell som indata. Resultatet är en klassificering av varje krav i kravmodellen som *giltigt*, d.v.s. att kravet är uppfyllt relativt systemmodellen, eller *falsifierbart*, att kravet inte är uppfyllt. Analysresultatet skickas sedan till uppdragsgivaren för vidare bedömning. I praktiken får man dock göra vissa modifieringar från den förenklade processbeskrivningen ovan. Dels kan bevisningen ta så pass lång tid att det är mer praktiskt att endast analysera enskilda krav eller grupper av krav åt gången. Dels kan analysen avslöja felaktigheter i system- och kravmodell vilket innebär att modelleringsarbetet måste itereras även under analysfasen.

9.1 Motmodeller och strömvägar

Om bevismotorn klassificerar ett krav som giltigt så är analysarbetet avslutat för just det kravet. Om kravet istället är falsifierbart så påbörjas arbetet med att försöka förstå orsaken i systemet till att kravet inte är uppfyllt. Ett viktigt hjälpmedel för denna analys är den s.k. *motmodellen* för kravet som bevismotorn producerar för alla falsifierbara krav. Motmodellen består av en fullständig listning av värdet för alla variabler i systemmodellen i varje tidssteg som bevismotorn sökt igenom. För att klargöra vad detta innebär bör man säga något om hur bevismotorn bär sig åt för att finna en motmodell. Bevismotorn startar alltid sökningen i initialtillståndet, d.v.s. det tillstånd där alla reläerna befinner sig i sina normallägen. Sedan simuleras att systemet förändras i tiden genom att tillåtna tillståndsövergångar äger rum, d.v.s. reläomslag som är möjliga enligt systemmodellen. I varje tidssteg kontrolleras om det undersökta kravet är uppfyllt. Sökningen är fullständig i den meningen att alla möjliga tillståndsövergångar i systemet kontrolleras. Om bevismotorn finner ett tidssteg där kravet inte är uppfyllt avslutas den och producerar motmodellen som alltså kan sägas innehålla hela historien fram till det tidssteg där kravet är falskt. Den första versionen av motmodellen innehåller värden för samtliga reläer i systemet. Detta är mer information än som behövs för att förstå varför ett utvalt krav är falsifierbart. En automatiserad filtrering av motmodellen utförs därför för att välja ut de reläer som är relevanta för kravet.

Låt oss anta att vi, i en fiktiv systemmodell, vill bevisa kravet:

```
X(D364_S) -> (H364_F & S364_F)
```

Nedan visas ett exempel på en tänkbar motmodell för detta krav. Kravet är falskt i motmodellen därför att X(D364_S) är sann i tidssteg 4 (operatorn *X* pekar här framåt mot tidssteg 5) men H364_F är falsk i tidssteg 4, vilket motsäger kravet.

Relä/Tid	1	2	3	4	5
D364_S	0	0	0	0	1
H364_F	0	0	0	0	-
S364_F	0	0	0	1	-

Tabell 3 Motmodell

Med hjälp av kravformuleringen och den filtrerade motmodellen är det möjligt att analysera orsaken till varför kravet är falskt. Ibland upptäcks att systemmodell eller kravformulering är inkorrekt. Efter korrigeringar och förnyad körning kan man visa att kravet trots allt var giltigt. I andra fall måste man ta hjälp av vana projektörer för att förstå motmodellen, som oftast kan avgöra om avvikelsen är säkerhetskritisk och föranleder korrigeringar i kretsritningarna. Ofta kan man behöva mer översiktlig in-

formation för att förstå orsakerna till att ett krav är falsifierat. Eftersom alla kraven schematiskt har formen *spole* -> *villkor*, är det klargörande att söka i kretsritningen efter spolen, och utifrån motmodellen avgöra vilken strömväg som är aktiverad i det falsifierade tidssteget. Sammanfattningsvis analyseras därför ett falsifierat krav utifrån följande indata:

- kravformulering
- motmodell
- strömsättningsväg för spole i motmodellen.

9.2 Analys av hårdvarufel

Analyserna inleds med att försöka bevisa att kraven är uppfyllda i normalmodellen, d.v.s. i den systemmodell där all hårdvara antas fungera korrekt. Då detta är gjort, och man därigenom har försäkrat sig om att systemet är logiskt korrekt, genomförs analysen igen, men med den extra möjligheten att något relä felar. Om man nu upptäcker ett falsifierat krav kan man alltså lokalisera exakt ett hårdvarufel, ett så kallat enkelfel, som leder till att kravet inte uppfylls. Genom att tvinga just detta enkelfel att inte inträffa och genomföra en ny analys kan man undersöka om det finns fler enkelfel. På så vis kan man finna alla enkelfel som vart och ett medför att kravet inte blir uppfyllt.

Efter att ha funnit alla enkelfel skulle man kunna tillåta att två reläer felar samtidigt och med samma teknik som ovan kan identifiera samtliga dubbelfel. I hittills genomförda CST-verifieringar har dock endast enkelfelsanalys utförts.

10 Referenser

[1] *Prover SL, native file format description*, Prover Technology AB.
[2] *Extractor 3.0, Användarmanual,* Prover Technology AB, ILE-03-SUM, 2008. Finns på IDA (Investering Mitt Stockholm, Stråk 22, Verktygslåda Cst).
[3] *Extractor, Tillämpningar*, Prover Technology AB, 2006-03-07.
[4] *Prover iLock Verifier,* produktinformation, http://www.prover.com/products/prover_ilock
[5] *Uttryck i förreglingstabeller*, PM, Banverket, BRÖBE, Göran Rönn, 2005-10-03.
[6] *Älvsjö, etapp Isärdragning – formell verifiering – kommentarer*. Banverket, BRÖBE, Göran Rönn, 2003-11-21.
[7] *Automatisering av kodning för formell granskning*, Uppsala Universitet, Örjan Erikssson, november 2003.
[8] *Uttryck i förreglingstabeller*, *översättning*, PM, Banverket, BRÖBE, Göran Rönn, 2005-10-03.
[9] *Eliminering av överkrav i signaleringsplaner*, PM, Banverket, BRÖBE, Göran Rönn, 2004-12-15.
[10] *Stockholm södra – formell verifiering – kommentarer*, Banverket, BRÖBE, Göran Rönn, 2002-05-21.
[11] *Formell verifiering av CST ställverk, Metodik II, fördjupning,* Prover Technology AB, 2010.