

Sammanfattning av deluppdrag

Rapporter från delprojekt Struktur & IT under perioden juni - oktober 2001
Lars Harms-Ringdahl, Lena Kecklund, Sven-Gunnar Krave och Peter Sjöquist.

1. Uppdrag och leverans

Inledning

Detta deluppdrag innefattar flera olika uppgifter, som har kopplingar till varandra. Denna summering ska knyta ihop dessa olika delar.

Deluppdrag

En specifikation av deluppdrag har gjorts utifrån de preliminära beskrivningarna vid Lidingöseminariet i maj 2001. Enligt projektledningen skulle arbetet i TRI fokusera på "Funktionella krav" (FK). Deluppdragen gällde:

1. Strukturer – presentation av olika förslag avsedda som underlag för slutligt beslut
2. Bedömning av norsk riskanalys och dess användning i TRI
3. Förslag till mall för riskbedömning "SORIR – FK"
4. MTO-perspektiv på TRI.

Efter samtal med och önskemål från regelgruppen inkluderades ett deluppdrag, som var inriktat på att:

5. Pröva en tillämpning som innebar en strukturering utifrån ett helhetsperspektiv.

Arbetets genomförande

Arbetet har genomförts i flera olika samarbeten. Deluppdrag 5 har gjorts ihop med Erik Hedlund och Margareta Lövgren från Regelgruppen. Ulf Pålsson har deltagit i uppgiften 1, och Ingemar Pålsson i uppgiften 2.

Leveranser

Leveransen omfattar följande rapporter som levererats på projektplatsen:

1. Strukturer i TRI-projektet - Version 1, L Harms-Ringdahl och L Kecklund, 2001-10-01.
2. Användning av existerande riskanalyser i TRI-projektet. L Harms-Ringdahl, 2001-10-08.
3. Bedömning av funktionella krav – SORIR-FK. L Kecklund och L Harms-Ringdahl, 2001-10-08.
4. MTO-perspektiv på TRI - Version 1. L Kecklund, 2001-10-18.
5. Struktur för Trafiksäkerhet och Funktionella Krav. L Harms-Ringdahl, E Hedlund, L Kecklund, och M Lövgren. 2001-09-28.

Alla överenskomna specifikationer har enligt vår bedömning uppnåtts, trots att en extra uppgift ihop med regelgruppen tillkommit.

2 Om delrapporterna

Strukturer i TRI-projektet

Materialet innehåller en presentation av olika sätt att strukturera säkerhetsarbete, handböcker etc. Den ger exempel på drygt 20 olika sätt att strukturera. Deluppdraget är avsett att ge underlag för att fatta beslut om det fortsatta TRI-arbetet.

Ett huvudproblem är att järnvägssäkerhet är ett stort och komplext område. Det finns inga enkla och självklara sätt att beskriva och systematisera detta. Det kan krävas olika strukturer för olika personalgrupper och aktörer, och det är angeläget att TRI-projektet kan hantera dessa olika behov. Den vanligaste inriktningen har varit att prioritera regler för fotfolket. Enligt vår mening är det också väsentligt att noggrant beakta ansvar och samspel mellan organisationer och företag.

För TRI behövs ett beslut, om hur grundstrukturen ska se ut. Det har inte varit vår avsikt presentera "det bästa" förslaget till lösning. Det finns fördelar och nackdelar med olika varianter som måste värderas mot varandra. Förslagsvis kan en särskild arbetsgrupp bedöma för- och nackdelar med olika förslag mot den kriterielista som presenteras i rapport nr. 1. Valet av struktur får stora konsekvenser för arbete och kostnader i en förvaltning av en framtida TRI.

Användning av riskanalyser

Riskanalysen från norska TRJ är som helhet inte direkt överförbar till TRI (se rapport nr. 2). Däremot kan beskrivningar och kategoriseringar användas på flera sätt i TRI-arbetet. Den mest uppenbara nyttan är att använda de omfattande och systematiska tabellerna och felträden för kontroller och kompletteringar.

Man bör från svensk sida inte satsa på begreppet "säkerhetskritisk funktion" i Sverige, av flera olika skäl. Om man däremot tolkar om "säkerhetskritisk funktion" till "viktig säkerhetsfunktion", finns det goda möjligheter till direkta jämförelser mellan norskt och svenskt material.

En annan slutsats är att det fortfarande finns behov av att göra riskanalyser på systemnivå och på förändringar i det svenska säkerhetsarbetet. Detta kan inte ersättas helt av norska och engelska riskanalyser.

Genomgången av den norska riskanalysen, liksom det engelska materialet, indikerar att det finns möjlighet till klara samordningsvinster. Man får ömsesidig nytta av olika riskanalyser, och vidare vore det intressant med en harmonisering av klassificering av gemensamma parametrar.

SORIR-FK

En översikt av olika parameterar etc. som behöver ingå i bedömningen och skrivandet av funktionella krav har gjorts i rapport 3. Slutlig utformning och omfattning av SORIR-FK kan göras då arbetsmetoden för regelskrivningen har fastställts för att få de olika delarna att på bästa sätt passa in i varandra och för att undvika att man gör onödigt arbete.

För att få en rationell hantering av SORIR bör man ha en databas och arbeta med klassificeringar direkt in i denna. Detta ger också möjlighet att stuva om och ändra strukturer. Det passar bättre att bedöma funktionsresurser än funktionella krav i SORIR-FK och man uppnår i princip samma syfte.

MTO-perspektiv på TRI

I rapport 4 finns summeringar av olika MTO-aspekter, bland med erfarenhet från TRAIN-projektet. Specifikt mot slutanvändaren måste man även se till att denne förstår syfte och innebörd i regeln, hur och i vilka situationer den ska användas, vilken risk som den ska kontrollera och i vilket sammanhang den ska användas. Regeltexten ska även ge underlag för att kunna fatta beslut i de situationer där det inte finns en exakt tillämplig regeltext (understödja användarens situationsmedvetande).

I ett MTO-perspektiv i TRI-arbete måste man tydliggöra regelverkets roll i styrningen av säkerheten och kunna kommunicera detta till att användaren. Dessutom måste frågor som berör ansvarsförhållanden mellan olika företag och organisationer tydligt klargämmas.

Struktur för trafiksäkerhet och funktionella krav

En modell och metodförslag har utvecklats och testats. I en särskild test på delområdet "Kommunikation" identifierades cirka 60 funktionella krav. En grov uppskattning pekar på 2000 FK. Detta innebär att FK får inte vara alltför detaljerade p.g.a. mängden.

Det blir viktigt att avgränsa och planera. Till detta hör att TRIs samspel mot omgivningen är väsentligt. En naturlig del i denna studie har varit att fundera över hur regelarbetet ska organiseras. Ett helhetsperspektiv behövs - och vilken modell som ska väljas är dock inte självklart. Oavsett vilken lösning man väljer krävs en rationell hantering av alla de olika element som ingår. Det gäller hur de hänger ihop och hur de påverkar varandra, samt att man inte tappar bort något väsentligt.

Vid struktureringen blir beslut om avgränsningar problematiska, relativt TRI-mallen, TRI föreskriften och andra regelverk. Förslag finns på hur man ska skilja ut de delar av styrningen av säkerheten som ligger utanför TRI, genom att SORIR-FK ger underlag för en enkel sortering.

Detta kräver en metodik och systematik, som ger uthållighet och möjligheter till parallell verksamhet som inte är alltför individberoende. Det finns också behov av spårbarhet och systematisk dokumentation.

Det blir ett komplext resultat med många parametrar och objekt. Lämpligt datorstöd behövs därför, annars blir det praktiska arbetet mycket tungrott. De beskrivna principerna kan ge stöd för uppdelning i lämpliga moduler, som i vårt exempel med "kommunikationspaketet".

Även om en metod förväntas ge en konsekvent bild, så behövs en noggrann bevakning av kvalitetsfrågor. Det räcker inte enbart att göra en bedömning av de regler eller FK som tagits fram. Exempelvis borde man gå igenom hela SÄO med kringföreskrifter (t

ex växlingsinstruktion och bromsföreskrifter) systematiskt för att se till att man inte har missat något.

3 Sammanfattning och slutsatser

Strukturering av material

Det finns många alternativa strukturer för regelsystem, funktionella krav etc. Det är väsentligt att man för TRI väljer en bra lösning, och att kraven på en lösning blir tydliga. Teman för viktiga kvalitetskriterier har föreslagits.

Av existerande strukturer verkar de engelska bäst, genom att de har en tydlig systematik och god täckningsgrad. Den metodik som finns i rapport 5 överensstämmer väl med denna både när det gäller modell och indelning i olika områden.

Stor datamängd

I rapporterna 1, 2 och 5 finns observationer av datamängder, vilket kan gälla antal regler och funktionella krav. Några exempel på värden är:

- Norska riskanalysen indikerar att antalet säkerhetskritiska funktioner är mellan 200 och 600. (Detta är en delmängd av alla säkerhetsfunktionerna.) (rap. 2).
- I rapport 5 pekar en preliminär uppskattning på 2000 funktionella krav (FK).
- I "kubmodellen" (rap. 1) ligger antalet element ("subblock") mellan 700 och 7 700. För varje element kan det finnas flera FK, å andra sidan kan ett antal subblock vara tomma.
- I det engelska materialet (rap.1) finns cirka 100 "Top controls", som i sin tur innehåller åtskilliga element. Det finns också mera konkreta "Safety measures", som sagts vara cirka 2000 till antalet.
- I sakregistret till svenska SÄO finns ca 1500 ord, vardera med ett antal hänvisningar.

Den stora datamängden visar att det behövs en god systematik för att hantera dessa och inte tappa bort något väsentligt.

Tidsaspekter och planering

Vid diskussioner av rapporterna i delprojektet har det blivit naturligt att ta upp frågor om planering och tidsåtgång.

I TRI-projektets planering är det viktigt att beakta mängden data. De gjorda uppskattningarna (eller något annat underlag) ger förutsättningar att bedöma tidsåtgång och behov av resurser. En god systematik kan ge stöd att bedöma tider, och att välja rimliga utsnitt som man ändrar reglerna för - man kan inte ändra allt samtidigt.

För att uppnå en godtagbar säkerhetsnivå för den slutliga produkten behövs tid och planering för MTO-granskning, riskanalyser och tester. Detta kan kräva extra mycket resurser om man inte har en tydlig och systematisk metodik från början.

En annan väsentlig aspekt är att inte riskera att delar av TRI underkänns, vilket kan medföra väsentlig tidsfördröjning.

Ett systematiskt arbetssätt

Frågor om systematik och de olika momenten i TRI-arbetet har dykt upp i alla fem delrapporterna. Exempel på teman som gäller behovet av en god systematik är:

- Att inte äventyra nuvarande säkerhetsnivå.
- Att kunna hantera mängden data för att ge ett bra urval och möjligheter till reduktion av antalet regler.
- Att täcka hela området, så att inte någon väsentligt del försvinner.
- Att tillse att reglerna är av tillräcklig kvalitet för att styra säkerheten, att det inte finns luckor.
- Att ge klara gränssnitt mellan gemensamma regler, branschregler, mellan företag etc.
- Att ha systematiska arbetsmetoder kan minska mängden fel och därmed minska behovet av testning och ge en snabbare tillämpning.

I rapport 5 finns en skiss på systematiskt arbetssätt. Även om den inte är helt färdig, kan de fungera som diskussionsunderlag för att finna en tillräckligt bra lösning.

Viktiga aspekter

Ett annat väsentligt kvalitetskrav på TRI som kommit från flera håll, är att man behöver finna en struktur som på ett rationellt sätt kan hantera kommande ändringar av regelverk. Det gäller både nationellt och internationellt initierade ändringar.

I delprojektet har vi dragit slutsatsen att internationellt samarbete är väsentligt. Det gäller engelska och norska pågående utvecklingsarbeten. Det finns mycket att lära, och kan ge möjligheter att komma rätt från början, också i de förutsedda europeiska harmoniseringarna.

Säkerhet i det framtida järnvägssystemet

En aspekt som kan bli så självklar att den glöms bort, är den säkerhetsnivå som ska uppnås efter att regeländringarna är genomförda. Det är väsentligt att klargöra hur detta ska åstadkommas. Det finns behov att lyfta fram ansvaret för detta i TRI. Projektledningen har huvudansvaret, men hur bör det se ut för delprojekten??

En delfråga är hur man ska ge tilltro till att regelverket ger tillräcklig säkerhet, där kopplingarna till tester, värderingar av mellanresultat, riskanalyser, granskningsmetodik, och slutgranskning är viktiga och intressanta.

Några väsentliga aspekter att beakta:

- Organisationsfrågor, ansvar, och samspel mellan aktörer. Detta är en grundläggande aspekt ur ett MTO-perspektiv
- Det behövs riskanalyser, och beskrivning av vad de ska de täcka. De norska (och engelska) analyserna räcker inte för att täcka behovet i Sverige.
- Det finns risker med att göra stora och många förändringar på samma gång.
- Viktigt att ha god kvalitet på slutprodukten. (bl a att inte nya, oförutsedda ”luckor” uppstår)
- Slut användaren måste anse att slutprodukten har blivit bättre