DIKU (Datalogisk Institut Københavns Universitet)
8. februar 2012, EF

Notat til brug ved IC4 høringen: Folketingets Transportudvalg til møde med Atkins vedrørende review af IC4/IC2 den 9. februar kl 10.30-12.00 i Det Færøske Pakhus

Jeg har ved flere lejligheder siden 2008 udtalt mig kritisk om softwaresystemerne i IC4 togene og her specielt peget på problemerne med sammenkoblingen af togsættene. Systemerne synes alvorligt fejlbehæftede og mangelfuldt forstået af de som står for og leder IC4-projektet og systemudviklingen. Atkins og Transportministeriets IC4/IC2 Review i form af de 54 power-point sider fra 19. oktober 2011 (AT-PP) og den samtidige, men noget senere offentliggjorte, 122 siders baggrundsrapport (AT-BR) bekræfter desværre den beskrivelse. Det vil jeg kort underbygge ved tre nedslag i udvalgte meget vigtige oplysninger der er givet i rapporterne.

De tre områder jeg vil fokusere på er følgende:

1. Sammenkoblingen af togsættene.

2. Filtrering og nedklassificering af sikkerhedsalarmer der præsenteres for lokoføreren via den såkaldte "Integrated Diagnostic Unit".

3. Bremseproblemerne - det fejlbehæftede samspil mellem IC4-togenes computersystem (Train Computer Management System), hjulblokeringssystemet (WSP-systemet) og det danske sikkerhedssystem for tog, ATC (Automatic Train Control).

Til punkt 1: Om sammenkoblingen af IC4-togsæt siges i Baggrundsrapporten, side 34:

"To further our understanding of the coupling system, we requested the IC4 Project Team to arrange a coupling demonstration which we could witness both from the Driver's cab and from the ground. This took place at Århus ... with two test drivers who were thoroughly familiar with the operation of IC4 trainsets. During a sequence of 5 coupling and uncoupling operations in ideal conditions there were 2 failures to complete the coupling sequence and 2 failures to complete the uncoupling process, a 40% failure rate. Furthermore, each of the 4 failures exhibited a different failure mode and ***in none of the failed operations was the root cause of the failure known or understood.***

Dette viser, at hverken DSBs projektteam eller konsulenterne fra Atkins har overblik eller forståelse af de fejlmeddelelser, som gives via Train Computer Management Systemet (TCMS) - endda vedrørende en funktionalitet som i årevis har været fremhævet som helt central for nytteværdien af IC4-togene i den landsdækkende trafikbetjening.

En sådan mangelfuld forståelse står i skærende modsætning til erklæringen i AT-PP, p. 49 *"De grundlæggende komponenter og systemer i IC4 togsættene har ikke væsentlige tekniske problemer."*

og

"TCMS designet har den ønskede funktionalitet". (AT-PP p 25)

Lad mig underbygge fejlagtigheden i Atkins rapportens karakteristik af systemerne som værende grundlæggende i orden ved at citere ingeniør Finn Jensen, systemintegrator i DSBs IC4-projekt. I en 3 A4-sider lang artikel i "Ingeniøren" den 30. dec 2011 i en sektion benævnt "Hovedløs systemintegration" udtaler Finn Jensen følgende: *"De italienske konstruktører ... er begyndt fra bunden uden et klart billede af det samlede system og dets funktionalitet. De har stolet på, at de nok skulle kunne få tingene til at spille sammen i sidste ende ved hjælp af software-justeringer. Men det skulle vise sig at være en skæbnesvanger forhåbning."*

Til punkt 2: Filtrering og nedklassificering af sikkerhedsalarmer.

AT-BR p 36-37 beskriver følgende om filtrering og nedklassificering af alarmer:

"... there is one specific known problem with the Train Computer Management System and the Integrated Diagnostic Unit which is that a high level of A and B alarms are being generated ... and, in many cases, these are spurious or repeat alarms. However, as an A alarm [that is a "top level fault" my remark] *requires a Driver response it frequently results in a casualty. AnsaldoBreda has experienced similar problems elsewhere and has implemented a software filter to mitigate the problem and the same solution is proposed for IC4.*

The IC4 Project Team has identified all the A alarms which may require to be filtered out or down-graded to a lower alarm level and from this has devised a set of 10 rules for filtering which will be installed in Pack 2 as version 1.6. The Team is now developing version 2.0 of the software to contain 125 rules and implementation of this version should have a significant impact on IC4's operational reliability. The filter software has been developed so that the application of rules can be revised in the light of further operational experience without further changes to the software and DSB personnel have been trained by AnsaldoBreda to undertake this function."

Her kan vi i AT-BR i næsten ren form læse om hvordan man i DSB og Ansaldo-Breda med Atkins fulde velsignelse forfølger den hasarderede vej med "gradually changing critical testing acceptance criteria" endnu inden der er opbygget en fuld forståelse af systemernes funktionalitet, deres indbyrdes samspil herunder systemerne samspil med togmateriellet og omgivelserne i øvrigt (banelegeme, vejrforhold mv). Og sådant filtersoftware vil man lægge i hænderne på DSBs personel. Det er i modstrid med elementære principper for testning af "safety critical systems" - hvad der her i højeste grad er tale om.

Til punkt 3: Havarikommissionens foreløbige undersøgelser af 30. jan 2012 vedrørende IC4-togsæt der den 7. nov 2011 passerede signal i "Stop" ved Marslev har bl.a. afdækket følgende forhold:

"- IC4-togtypens hjulblokeringssystem (WSP-system) kan under meget glatte forhold ikke sikre mod hel/delvis hjulblokering af togets hjul

- hel/delvis hjulblokering vil medføre mangelfuld registrering af den faktiske tilbagelagte strækning ved bremsning under disse særlige forhold samt manglende registrering af den reelle hastighed

- hel/delvis hjulblokering kan medføre at sikkerhedssystemet (ATC) ikke kan sikre at toget bringes til standsning inden for sikkerhedsafstanden, dvs. før et farepunkt.

- på IC4 togsættet er den serielle forbindelse mellem togcomputer og ATC ikke etableret. En seriel forbindelse vil bl.a. sikre information til ATC-anlægget i tilfælde af akut nedskrivning af bremseprocent (tab af bremseevne) under bremsning."

Igen er der tale om fejl og mangler i togcomputeren (TCMS'en), hjulblokeringssystemet og samspillet til ATC-anlægget. Denne konstatering fremkommer her i 2012 efter at der har været stillet en række spørgsmål til netop disse forhold siden i hvert fald foråret 2009 af bl. a. Per Clausen (EL) og transportministeren har hver gang - på basis af oplysninger fra DSB - kunnet oplyse "at *DSB ikke har konstateret problemer med ATC systemet i forhold til IC4 togsættene*". Men Havarikommissionens undersøgelser har altså afdækket noget ganske andet.

Der har været en del fremme om glatte skinner som medvirkende årsag. Men her må det fremhæves, at Havarikommissionen nævner, at der omkring stedet for hændelsen kun er enkelte

træer, ingen skov, og at der i dagene efter den farlige hændelse alene er konstateret en begrænset mængde løvfald (*meget få blade*) på eller ved sporet.

Meget tyder for mig på, at der snarere er tale om aperiodiske systemfejl. Fejl som kun opstår under helt særlige betingelser, og som det kan være vanskeligt af afdække og udbedre. Det forekommer ikke helt sjældent i forbindelse med - som her - s*afety critical* realtidssystemer, i flere tilfælde med fatale ulykker til følge.

AT-PP giver visse indikationer i samme retning, fx p 24:

"Bremse-systemfejl er spredt over en række komponenter og tekniske årsager...

Bremse-computer kan være et spirende problem – yderligere analyse af fejlrapporter er påkrævet".

På denne baggrund må rejses *det røde stopsignal*: Det er nu tvingende nødvendigt med en tilbundsgående og uafhængig ekspertundersøgelse af IC4-togenes computersystemer.

Alt andet er fagligt uforsvarligt med de mange fakta, der foreligger til dokumentation af alvorlige fejl og mangler i systemernes funktion, deres pålidelighed og deres sikkerhed. Atkins-undersøgelserne er helt utilstrækkelige og har primært tjent til at blotlægge endnu flere fejl og mangler. Atkins-konsulenternes beroligende vurderinger og anbefalinger savner grundlag i deres egne faktiske beskrivelser.

Hvis de ansvarlige for IC4-togenes ibrugtagen i Danmark - i DSB, i Trafikstyrelsen, og i Transportministeriet - vælger at sidde de mange faresignaler vedrørende tilstanden af IC4-togenes computersystemer overhørig uden en grundig undersøgelse af den art, som jeg her har antydet, finder jeg det ansvarspådragende i tilfælde af en fatal IC4-ulykke.

Lektor Erik Frøkjær, forskergruppeleder
Datalogisk Institut, Søndre Campus
Københavns Universitet, Njalsgade 128
Bygning 24, 5. sal
DK-2300 København S

Tlf. DIKU: +45 3532 1456, Mobil: 45 4035 4275
email: erikf@diku.dk