Skjulte avhengigheter i signalsystemene?
- Hvordan unngå at togene kolliderer

Terje Sivertsen
Seksjonsleder Signal
Jernbaneverket Banedivisjonen
Teknikk, Premiss og utvikling

Skjulte avhengigheter i komplekse systemer,
SINTEF, 15 januar 2009

Lang vei fra start til mål

Start

Etablering av Jernbaneverkets krav

Fareidentifisering, risikoanalyser, fareanalyser
funksjonskravspesifikasjon, systemkravspesifikasjon,
systemsikkerhetskravspesifikasjon,
programvarekravspesifikasjon,
programvarearkitektur, programvaredesign, ...

Mål

Godkjent produkt/applikasjon

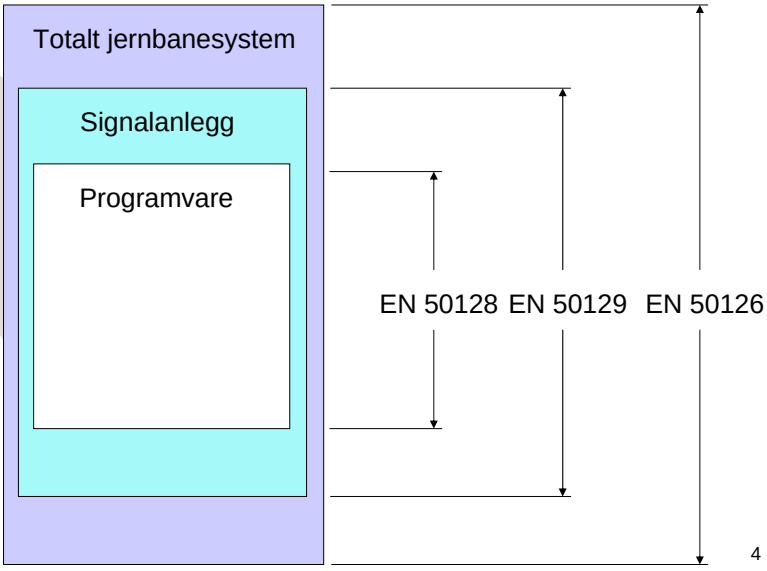
Drift og vedlikehold

2

... i tillegg kommer garantert endringer underveis

3

CENELECs sikkerhetsnormer



4

Sikkerhetskritiske funksjoner

- CENELECs sikkerhetsnormer forutsetter at sikkerhetskritiske funksjoner identifiseres og tilordnes tolerable farerater (THR)
- Innenfor signal opererer Jernbaneverket med fem grunnleggende sikkerhetskritiske funksjoner
- Eksempelvis skal et lyssignal *"vise korrekt signalbilde og gi korrekt informasjon til forriglingsutrustningen om signalets status"*
- THR for de ulike funksjonene er utledet fra dagens risikonivå
- Sikkerhetsintegritetsnivå (SIL) utledes fra THR i samsvar med CENELECs sikkerhetsnormer

5

Avhengigheter mellom sikkerhetskritiske funksjoner

- De ulike sikkerhetskritiske funksjoner er innbyrdes avhengige
- Sikkerheten knyttet til jernbanen som system avhenger av at fareratene knyttet til de sikkerhetskritiske funksjonene er lavere enn de tolerable fareratene
- Fareraten overvåkes kontinuerlig gjennom systematisk registrering og rapportering av sikkerhetsfeil
- Avvik fra THR kompenseres gjennom å innføre flere barrierer mot uønskede hendelser (MTO)

6

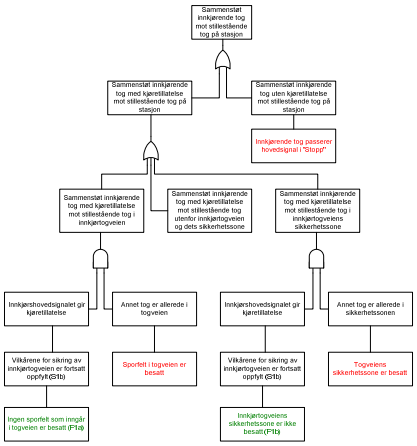
Tekniske regler og krav

- Signalsystemene utformes på basis av Teknisk Regelverk, kravspesifikasjoner og applikasjonsspesifikke data (skjematisk plan og forriglingstabell)
- Regler og krav har ofte lang historikk, og det kan være vanskelig å kjenne begrunnelsen
- Inngående kjennskap til fagområdet er nødvendig for å forstå hvordan de ulike reglene og kravene er relatert til hverandre og til de sikkerhetskritiske funksjonene

7

Analyse og verifisering

- Sikkerhetsanalyser og kravsporing bidrar til å underbygge kravene, forhindre uønskede effekter av endringer, og legge til rette for sikkerhetsbevisets demonstrasjon av oppfyllelse av krav
- En klar tendens internasjonalt å benytte formelle og semi-formelle spesifikasjonsteknikker
- Jernbaneverket benytter formelle metoder i verifiseringen av PLS-baserte sikringsanlegg



8

Programvaredesign

- Programvaredesignet for PLS-baserte sikringsanlegg dokumenteres gjennom funksjons- og designspesifikasjonene
- Består i hovedsak av Boolske likninger som definerer funksjonene (variablene) som skal beregnes, sammen med en spesifikasjon av beregningsrekkefølgen
- Samme programvaredesign brukes som basis for begge kanaler (PLS A og PLS B)
- Feil i programvaredesignet kan lede til feil i begge kanaler
- Divers analyse gjennom strukturert gransking og formell verifisering

9

Programkode

- Divers programmering for PLS A og PLS B
- Ulike programmeringsspråk
- Uavhengige programmeringsteam
- Design og verifisering utføres av ulike personer
- Effekten av diversitet usikker
- Programdesignet begrenser diversiteten
- Divers verifisering gjennom strukturert gransking og formell verifisering
- Verifiseringen kan utføres alternativt på kildekode eller objektkode

10

Andre aktuelle tiltak

- Alternative kravmodeller
- Divers programvaredesign
- Automatisert prosjektering
- Automatisert kodegenerering
- Ulik maskinvare for PLS A og PLS B
- Sertifiserte komponenter
- Økende grad av selv-overvåking
- Invarianter som dekker hele strekninger
- Forsterket formell verifisering
- Logganalyse

11

Oppsummering

- CENELECs sikkerhetsnormer er grunnleggende for fremskaffelsen av Jernbaneverkets signalsystemer
- Mange avhengigheter mellom regler, krav og funksjoner – ikke nødvendigvis skjulte men heller ikke nødvendigvis så godt synlige
- Sikkerhetsanalyser, kravsporing og formelle metoder viktige midler for å forhindre skjulte avhengigheter
- Effekten av divers programvareutvikling vanskelig å tallfeste
- Mange muligheter til ytterligere barrierer mot at tog kolliderer som en konsekvens av skjulte avhengigheter

12