Trafik- og Byggestyrelsen
Danish Transport and Construction Agency

Vejledning om godkendelse af systemer med software på jernbanen

Version 2 af 22. marts 2016

Forord

1. Generelt

Software (SW) indgår som en vigtig byggesten i jernbanens delsystemer. Delsystemernes sikkerhedsfunktioner baseres i høj grad på SW, og delsystemerne har ofte komplicerede grænseflader i sig selv og til andre delsystemer, som det fx er tilfældet mellem fast- og mobilt togkontrol. SW spiller således en vigtig rolle for jernbanesikkerheden.

Uanset om der er tale om ny SW, som skal udvikles fra bunden, eller eksisterende SW, som skal ændres, er det vigtigt at følge egnede processer hertil. Nærværende vejledning refererer til standarden EN50128:2011[1] og ISO/IEC 90003:2015, som netop beskriver anerkendte og egnede processer. Andre processer vil kunne anvendes i den udstrækning, som det er foreneligt med gældende lovgivning.

SW udviklings-, ændrings- og godkendelsesprocessen kan være forholdsvis kompliceret, og involvere mange forskellige roller og kompetencer, fx

- Projektledelsen
- SW-designeren
- Verifikatoren, jf. EN50128
- Validatoren, jf. EN50128
- Et bemyndiget organ (NoBo)
- En uafhængig assessor jf. EN50128 (ASR)
- En uafhængig assessor jf. CSM RA (AsBo)
- En infrastrukturforvalter eller jernbanevirksomhed

Nærværende vejledning er primært tiltænkt anvendt i jernbanevirksomheder og infrastrukturforvaltere, som via deres sikkerhedsledelsessystem (SLS) skal sikre sig, at nye delsystemer ikke tages i brug uden en ibrugtagningstilladelse, og at senere ændringer håndteres forsvarligt i overensstemmelse med gældende lovgivning.

Vejledningen understøtter bekendtgørelserne om ibrugtagningstilladelse for delsystemer i infrastrukturen og godkendelse af køretøjer med tilhørende vejledninger, og vedrører både SW som implementerer sikkerhedskrav, og SW der alene implementerer krav i TSIer eller NNTR[2], som ikke nødvendigvis er sikkerhedsrelaterede. Andre processer end dem der foreskrives i EN50128 og ISO/IEC 90003 kan være relevante for SW, der er udviklet for mange år siden. Vejledningen kan også anvendes i forbindelse med ændring i sådanne systemer. Se mere herom i kapitel 15 og eksemplet i bilag 2.

Hardware (HW) og SW ændringer kan være lige kritiske, og det kan komplicere risikostyringen, hvis der ændres i begge dele samtidigt. Nærværende vejledning fokuserer på rene SW ændringer. Vejledningen kan derfor ikke stå alene, men skal anvendes sammen med Trafik- og Byggestyrelsens øvrige vejledninger.

Software, der alene vedrører "security[3]", behandles ikke i nærværende vejledning. Såfremt "security" software er indeholdt i øvrig sikkerhedsbærende software, kan vejledningen bruges.

2. Formål

Formålet er at vejlede om hvordan jernbanevirksomheder, infrastrukturforvaltere og deres leverandører forventes at involvere sig i SW udvikling og ændringer heri, samt at vejlede i hvordan det undersøges om Trafik- og Byggestyrelsen skal involveres i godkendelsen.

[1] Tilsvarende standarder vil også kunne anvendes, herunder den tidligere udgave af EN50128. Det anbefales dog så vidt muligt at følge de nyeste standarder, da disse anses som 'best practice'. Se kapitel 15 ang. håndtering af systemer med SW som ikke er udviklet i henhold til en anerkendt praksis.

[2] NNTR står for en 'Notificeret National Teknisk Regel'.

[3] Med security SW menes SW, der beskytter mod, at uautoriserede personer, med onde hensigter, kan skaffe sig adgang til at ændre i software som vedrører jernbanesikkerhed.

3. Ændringshistorik

Version	Afsnit	Bemærkning
Foreløbigt udkast, af 23. oktober 2015	Alle	Fordelt til Branchepanelet for Jernbane
Version 1 af 28.2.2016	Alle	Opdateret på baggrund af reviews og kommentarer modtaget af branchepanelet
Version 2 af 22.3.2016	Bilag 3	Systemtegning indsat i forbedret opløsning.

Note: Trafik- og Byggestyrelsen ønsker at indhente erfaring med vejledningen. Kommentarer kan sendes til: info@tbst.dk

4. Hvordan læser man vejledningen

Kapitlerne læses bedst i kronologisk rækkefølge, da flere begreber løbende introduceres.

Forkortelser er forklaret i kapitel 5.

Referencer fremgår af kapitel 6. Der er brugt følgende syntaks for henvisninger til referencer; /x/, hvor x er den pågældende reference.

I kapitel 7 introduceres begrebet ”CSM systemet”, og i vejledningens figurer er CSM systemets grænseflade altid vist med en fed blå streg.

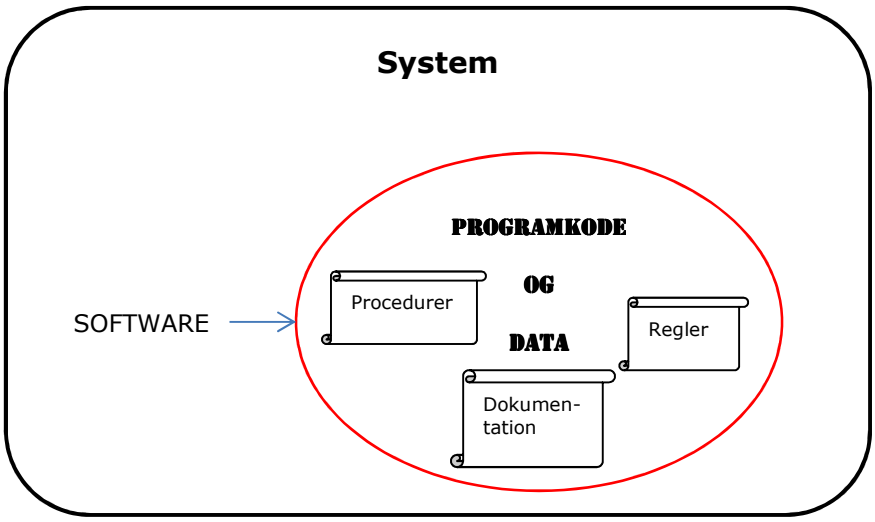
Indhold

Indledning

Software (SW) er fysisk set uhåndgribeligt, idet SW i det idriftsatte fysiske system er en fil indeholdende genereret programkode og data, som kun en computer kan læse og tolke.

SW er i standarden EN50128 defineret som: "Intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system".

Software er med andre ord altid noget der indgår i et fysisk system og medvirker i systemets funktioner. Dette er illustreret på Figur 1[4]:



Figur 1 SW er en del af systemet

Når et delsystem i det samlede jernbanesystem ændres, kan det medføre, at delsystemet skal recertificeres af NoBo/DeBo eller en køretøjssagkyndig, og samtidig skal CSM RA forordningen anvendes, hvor det indledningsvis skal undersøges, om ændringen er signifikant.

Kriterierne for afgørelse af signifikans i CSM RA forordningen er typisk rettet mod det fysiske system og dets integration i jernbanesystemet. Ved at anvende CSM RA processen er det muligt at identificere de CSM sikkerhedskrav (herunder SIL krav) som sikkerhedsfunktionerne skal implementere. CSM RA egner sig imidlertid ikke til at styre, hvilke utilsigtede konsekvenser en SW ændring kan have. Derfor er det nødvendigt at anvende en anerkendt praksis (fx EN50128) til at sikre, at softwaren udvikles, så sikkerhedskravene opfyldes.

Nærværende vejledning handler derfor om at beskrive ovenstående rammebetingelser, og hvordan det kan vurderes om en ændring i et system med SW:

- er signifikant jf. CSM RA og/eller
- skal certificeres af NoBo/DeBo/køretøjssagkyndig,

samt hvornår Trafik- og Byggestyrelsen skal inddrages.

[4]Ved procedurer, regler og dokumentation menes, procedurer, regler og dokumentation som vedrører software udvikling og implementering. Data, som anvendes af computeren, anses som "SW".

5. Definitioner og forkortelser i vejledningen

AsBo	Assessment body jf. CSM RA /3/.
ASR	Assessor jf. EN50128 /5/.
ASSR	Assessor jf. EN50129 /6/.
BEKxxx	Bekendtgørelse nr. xxx.
BUS	En BUS (ordet relaterer sig til det Latinske ord "omnibus", som betyder "for alle") er det kommunikationssystem som transmitterer data i en computer, eller mellem flere computere.
Computeren	Den hardware (HW), som består fx af komponenterne CPU, IO, Rack, BUS og den Memory, der indeholder programkode, data osv.
Configuration Manager	Den funktion hos SW leverandøren, der har ansvaret for Software Configuration Management i hht. EN50128. ”3.1.5, configuration manager: entity that is responsible for implementing and carrying out the processes for the configuration management of documents, software and related tools including change management”. Configuration Management er en administrativ aktivitet.
CPU	Central Processing Unit. Den kan også kaldes en centralenhed eller blot en processor.
CSM RA	EU forordning nr. 402/2013: Den fælles europæiske sikkerhedsmetode til risikoevaluering og –vurdering /3/.
CSM sikkerhedskrav	Krav til CSM-systemet, fastlagt vha. CSM RA. CSM RA, artikel 3: »sikkerhedskrav«: de nødvendige sikkerhedsegenskaber (kvalitative eller kvantitative, eller når det er nødvendigt, både kvalitative og kvantitative), for konstruktionen, drift (herunder driftsforskrifter) og vedligehold af et system med henblik på at opfylde lovbestemte eller virksomheders sikkerhedsmål«.
CSM-systemet	En funktionel enhed i delsystemet, som består af HW og SW med en eller flere bestemte SW funktioner placeret enten i et køretøj eller i infrastrukturen.
DeBo	Udpeget organ.
Delsystem	Resultatet af jernbanesystemets opdeling i strukturelt og funktionelt definerede delsystemer, som angivet i IOD bilag II.
DV 29bis	Kaldenavn for (2014/897/EU): Kommissionens henstilling af 5. december 2014 om forhold vedrørende ibrugtagning og anvendelse af strukturelt definerede delsystemer og køretøjer efter reglerne i Europa-Parlamentets og Rådets direktiv 2008/57/EF og 2004/49/EF. /7/.
ECM	Entity in Charge of Maintenance.
Forslagsstiller	Jf. CSM RA artikel 3, 11) kan forslagsstiller være en af følgende: a) en jernbanevirksomhed eller jernbaneinfrastrukturforvalter, som implementerer risikokontrolforanstaltninger i henhold til artikel 4 i direktiv 2004/49/EF b) en enhed med ansvar for vedligeholdelse, som implementerer foranstaltninger i henhold til artikel 14a, stk. 3, i

	direktiv 2004/49/EF c) ordregivere eller fabrikanter, som opfordrer et bemyndiget organ til at anvende EF-verifikationsproceduren i overensstemmelse med artikel 18, stk. 1, i direktiv 2008/57/EF, eller et organ, der er udpeget i henhold til artikel 17, stk. 3, i samme direktiv d) en, der ansøger om tilladelse til at tage strukturelt definerede delsystemer i brug.
HW	Hardware er en generel betegnelse for den mekanik og elektronik, der indgår i et system.
IO	Input/Output.
IOD	Interoperabilitetsdirektivet. /8/.
IM	Infrastrukturforvalter.
Konfigurationsansvarlig	Den funktion i jernbanevirksomheden eller infrastrukturforvalteren, der er ansvarlig for at implementere og gennemføre konfigurationsstyringsprocesser for den HW/SW der anvendes i driften, i overensstemmelse med virksomhedens sikkerhedsledelsessystem. Konfigurationsstyring er en administrativ aktivitet.
Modul	I forbindelse med software er et modul en afgrænset del af softwaren svarende til 'Software components' i EN50128. Betegnelsen 'modul' anvendes også som en verifikationsprocedure jf. /12/.
NNTR	Notificeret National Teknisk Regel.
NoBo	Bemyndiget organ.
PIS	Passagerinformationssystem.
Program / Programkode	Den del af SW, der findes i computeren.
QMS	Kvalitetsstyringssystem (Quality Management System) hos fabrikanten.
Sikkerhedsfunktion	Defineret i EN50128: "A function that implements a part or whole of a safety requirement." En sikkerhedsfunktion kan afhænge af SW, HW, procedurer og menneskelig indgriben. Sikkerhedsfunktioner kan være interne i CSM systemet, eller virke over CSM systemets grænseflader.
RU	Jernbanevirksomhed.
SIL	Safety Integrity Level. EN50126: "One of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems". SIL niveauet (0-4) er udtryk for den tillid, som man kan have til en sikkerhedsfunktion på systemniveau virker efter hensigten. En funktion med SIL = 0 kan man ikke have stor tillid til virker efter hensigten, mens man kan have stor tillid til, at en funktion med SIL = 4 virker korrekt. Sikkerhedsfunktioner implementeres typisk med bidrag fra både HW og SW.
Software safety integrity level (SSIL)	"Classification number which determines the techniques and measures that have to be applied to software". Se også SIL. Den del af systemets Safety Integrity Level som er tildelt SW. Ofte er SSIL det samme som SIL, men i vejledningen er det

	holdt adskilt.
SLS	Sikkerhedsledelsessystem hos jernbanevirksomheden/infrastrukturforvalteren.
SVR	Sikkerhedsvurderingsrapport.
SW	Software: "An intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system".
SW sikkerhedsfunktion	Hermed menes softwarens bidrag til den samlede sikkerhedsfunktion, som kan inkludere mekanik, el-teknik, mm..
SW kravspecifikation	Defineret i EN50128, 7.2.4.2: The Software Requirements Specification shall express the required properties of the software being developed. These properties, which are all (except safety) defined in ISO/IEC 9126 series, shall include: a) Functionality (including capacity and response time performance), b) Robustness and maintainability, c) Safety (including safety functions and their associated software safety integrity levels), d) Efficiency, e) Usability, f) Portability.
System	Almen betegnelse for noget, der kan afgrænses til at være indeholdt i 'systemet'. Det kan dække over meget afhængig af konteksten.
TSI	Teknisk Specifikation for Interoperabilitet.
Validator	Enhed med ansvar for valideringen.
Verifikator	Enhed som er ansvarlig for en eller flere verifikationsaktiviteter.

6. Referencer

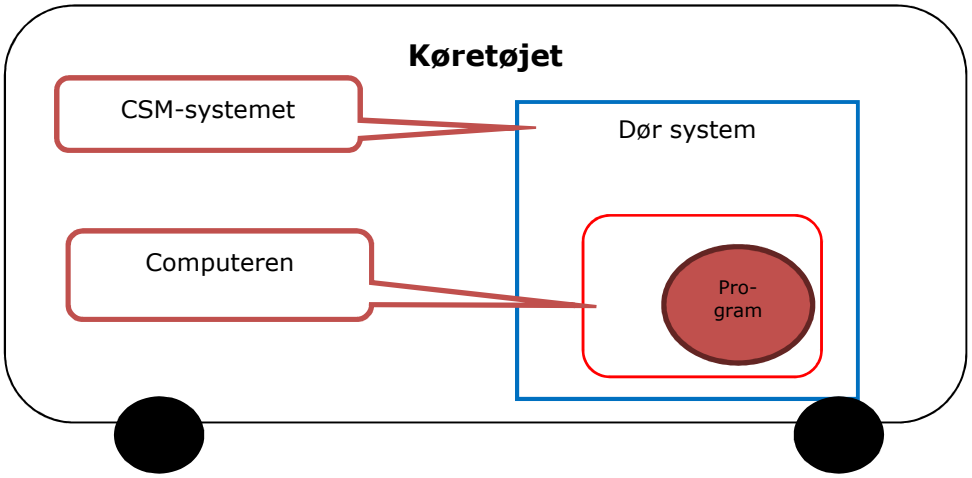
/1/ BEK653	Bekendtgørelse nr. 653 af 8. maj 2015 om godkendelse af køretøjer på jernbaneområdet, ændret ved bekendtgørelse nr. 859 af 07/07/2015 om ændring af bekendtgørelse om godkendelse af køretøjer på jernbaneområdet.
/2/ BEK661	Bekendtgørelse nr. 661 af 8. maj 2015 om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen, ændret ved bekendtgørelse nr. 864 af 07/07/2015 om ændring af bekendtgørelse om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen.
/3/ CSM RA	Kommissionens gennemførelsesforordning (EU) Nr. 402/2013 af 30. april 2013 om den fælles europæiske sikkerhedsmetode til risikoevaluering og –vurdering og ophævelse af forordning (EF) nr. 352/2009, som ændret ved Kommissionens gennemførelsesforordning (EU) 2015/1136 af 13. juli 2015 om ændring af gennemførelsesforordning (EU) nr. 402/2013 om den fælles sikkerhedsmetode til risikoevaluering og – vurdering.
/4/ EN50126	DS/EN 50126-1:1999, 1. udgave 2014 10-10: Jernbaneanvendelser – Specifikation og eftervisning af pålidelighed, tilgængelighed, servicerbarhed og sikkerhed (RAMS) – Del 1: Grundlæggende krav og generisk fremgangsmåde indeholdende corrigendum fra maj 2010. (Standarden er under revision).
/5/ EN50128	DS/EN 50128:2011 og DS/EN 50128/AC:2014: Jernbaneanvendelser – Kommunikations-, signal- og processystemer – Programmel for styre-og sikkerhedssystemer.
/6/ EN50129	DS/EN 50129 + AC:2010, 1. udgave, 2014-10-10: Jernbaneanvendelser – Kommunikations-, signalgivnings- og databehandlingssystemer – Sikkerhedsrelaterede elektroniske systemer til signaludstyr.
/7/ ”DV29bis”	Kommissionens henstilling af 5. december 2014 om forhold vedrørende ibrugtagning og anvendelse af strukturelt definerede delsystemer og køretøjer efter reglerne i Europa-Parlamentets og Rådets direktiv 2008/57/EF og 2004/49/EF.
/8/ IOD	Europa-Parlamentets og Rådets direktiv 2008/57/EF af 17. juni 2008 om interoperabilitet i jernbanesystemet i Fællesskabet, med senere ændringer.
/9/ IEC 61508	Standard fra "the International Electrotechnical Commission" omhandlende "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)".
/10/ ISO/IEC 90003	DS/ISO/IEC 90003:2015. Softwareudvikling – Retningslinjer for anvendelse af ISO 9001:2008 til computersoftware.
/11/ IOD gennemførelsesbekendtgørelse	Bekendtgørelse nr. 1281 af 19. november 2015 om interoperabilitet i jenbanesystemet
/12/ Afgørelse om verifikationsmoduler	Kommissionens afgørelse af 9. november 2010 om de moduler til procedurer for vurdering af overensstemmelse og anvendelsesegnethed og for EF-verifikation, der skal benyttes i tekniske specifikationer for interoperabilitet, som er vedtaget i medfør af Europa-Parlamentets og Rådets direktiv 2008/57/EF (2010/713/EU).

Håndtering af software

7. Introduktion

Som beskrevet i indledningen eksekveres SW i en computer, der indgår i den funktionelle enhed, som i denne vejledning er kaldt 'CSM-systemet'. Dette indgår i en større systemsammenhæng i det overordnede delsystem i jernbanen.

At systemet, der indeholder SW, kaldes for CSM-systemet skyldes, at det er den enhed, der løser funktioner ved hjælp af SW og derfor bør håndteres i henhold til vejledningen. Dette kan illustreres med følgende eksempel for et jernbanekøretøj, hvor CSM-systemet er et dørstyringssystem. CSM-systemet er her hele den funktionelle enhed indeholdende døre, låsemekanismer, klemsikringer, overvågning, manøvrering, computeren osv.:



Figur 2 Systemopdeling

Computeren er den del af CSM-systemet, der indeholder softwarens programkode. Programkoden findes i computerens memory. HW og SW skal i denne sammenhæng ses som lige kritiske, hvad enten der foretages ændringer i SW eller HW, men denne vejledning er primært beregnet på ændringer af SW.

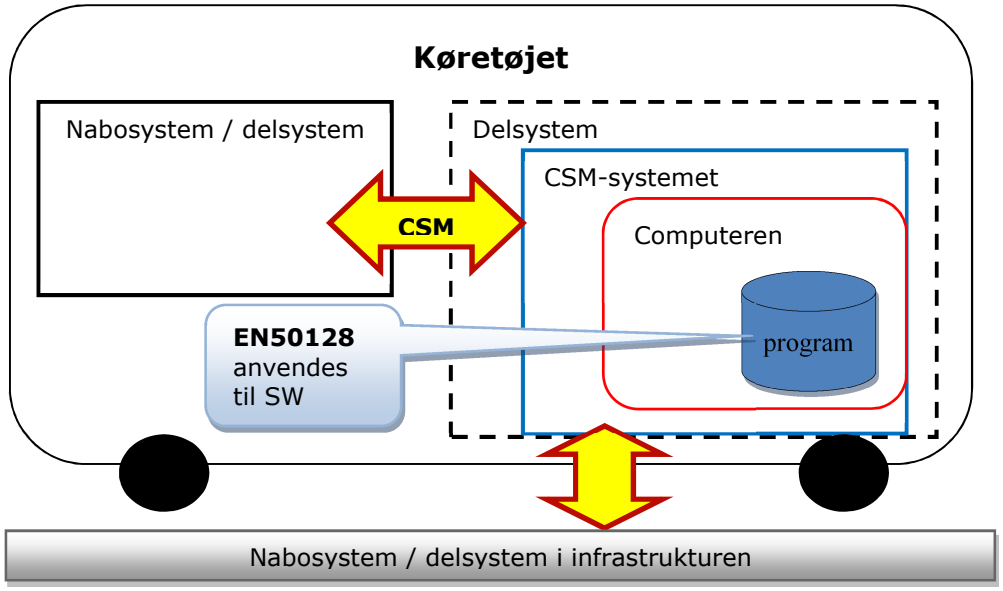
Indholdet i systemdefinitionen for CSM-systemet, indeholdende computeren, er nærmere beskrevet i kapitel 10.

Når CSM-systemet er defineret, lægger nærværende vejledning op til, at følgende skal vurderes i forbindelse med en ændring:

1) Det skal vurderes, om SW-ændringen er en signifikant ændring af CSM-systemet (Kapitel 13)
2) Det skal vurderes, om SW-ændringen i computeren er "kritisk". Resultatet af denne vurdering vil være, at ændringen enten er 'major' eller 'minor' (Bilag 1)
3) Om ændringen påvirker allerede udstedte verifikationsattester[5] og/eller kan betragtes som fornyelse/opgradering (Kapitel 11)

[5] Verifikationsattester udstedt af et NoBo, DeBo, eller en køretøjssagkyndig.

Sammenhængen mellem standarder, CSM RA og begreber
I det tilfælde hvor ændringen er vurderet signifikant eller ændringen er omfattet af en TSI/NNTR, der foreskriver, at man skal bruge CSM RA, medfører det, at forslagsstiller skal følge CSM RA. For stillingstagen til signifikans henvises til denne vejlednings kapitel 13. Når CSM RA følges, og SW også skal udvikles/ændres, kan processerne herfor illustreres som vist på Figur 3 nedenfor:



Figur 3 CSM RA og EN50128 processer

Figur 3 illustrerer, at programmet afvikles i computeren (rød kasse), der indgår i systemfunktionen for CSM-systemet (blå kasse), der igen indgår i det overordnede delsystem (sort stiplet).

Computeren (inkl. programmet) er en del af CSM-systemet, der igen er en del af delsystemet.

Ifølge DV 29bis kan CSM RA bruges til den sikre integration af delsystemer og mellem elementer i delsystemet herunder sikker integration med infrastrukturen (gule pile). Det fremgår af kapitel 10, hvordan systemdefinitionen for dette kan laves.

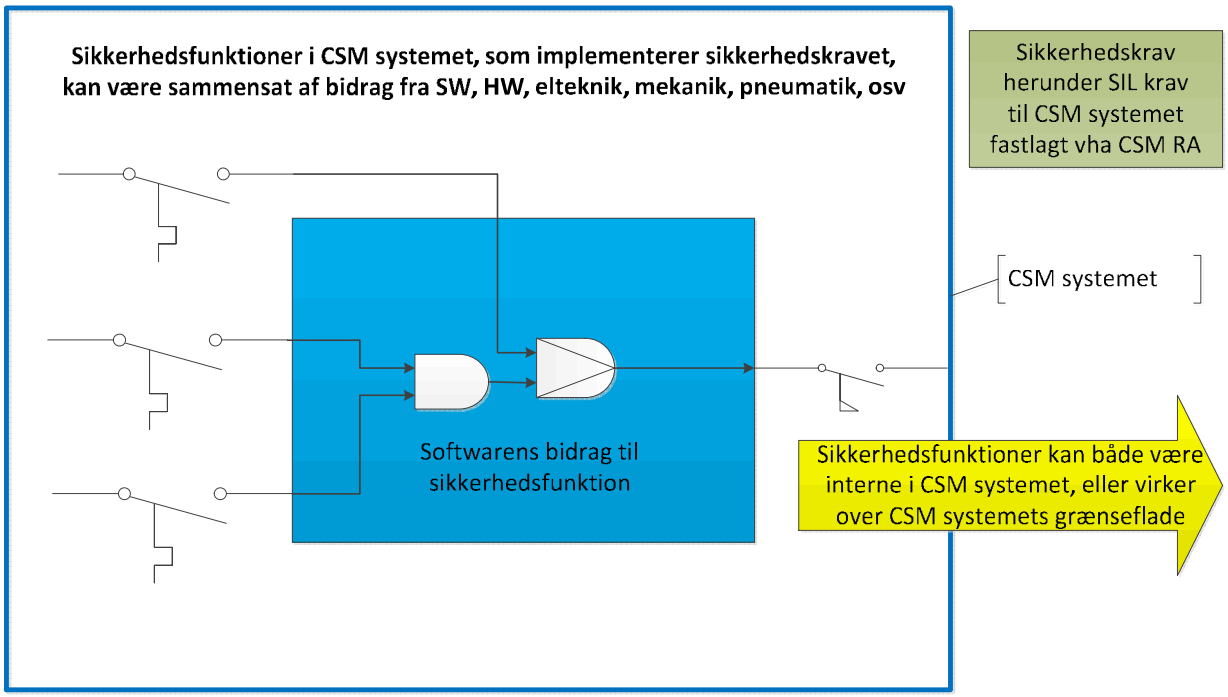
CSM RA kan således anvendes til at risikostyre alle farer relateret til grænsefladerne og den sikre integration.

EN50128-standarden er en anerkendt metode, der kan anvendes for at kontrollere farer forbundet med SW udvikling, og dermed hjælper til at gøre SW sikker at anvende. EN50128 tager udgangspunkt i, at der er udarbejdet sikkerhedskrav på systemniveau, i det efterfølgende kaldt "CSM sikkerhedskrav".

CSM sikkerhedskravene opstilles ved at anvende CSM RA[6]. Systemarkitekturen og fordeling af sikkerhedskravene (eng."apportionment"), fastlægges samtidigt i den iterative CSM proces.

[6] Ofte følges EN50126 også.

Nedenstående Figur 4 illustrer sammenhængen mellem CSM sikkerhedskrav, sikkerhedsfunktioner og SW funktioner.



Figur 4 Softwarens bidrag til den samlede sikkerhedsfunktion.

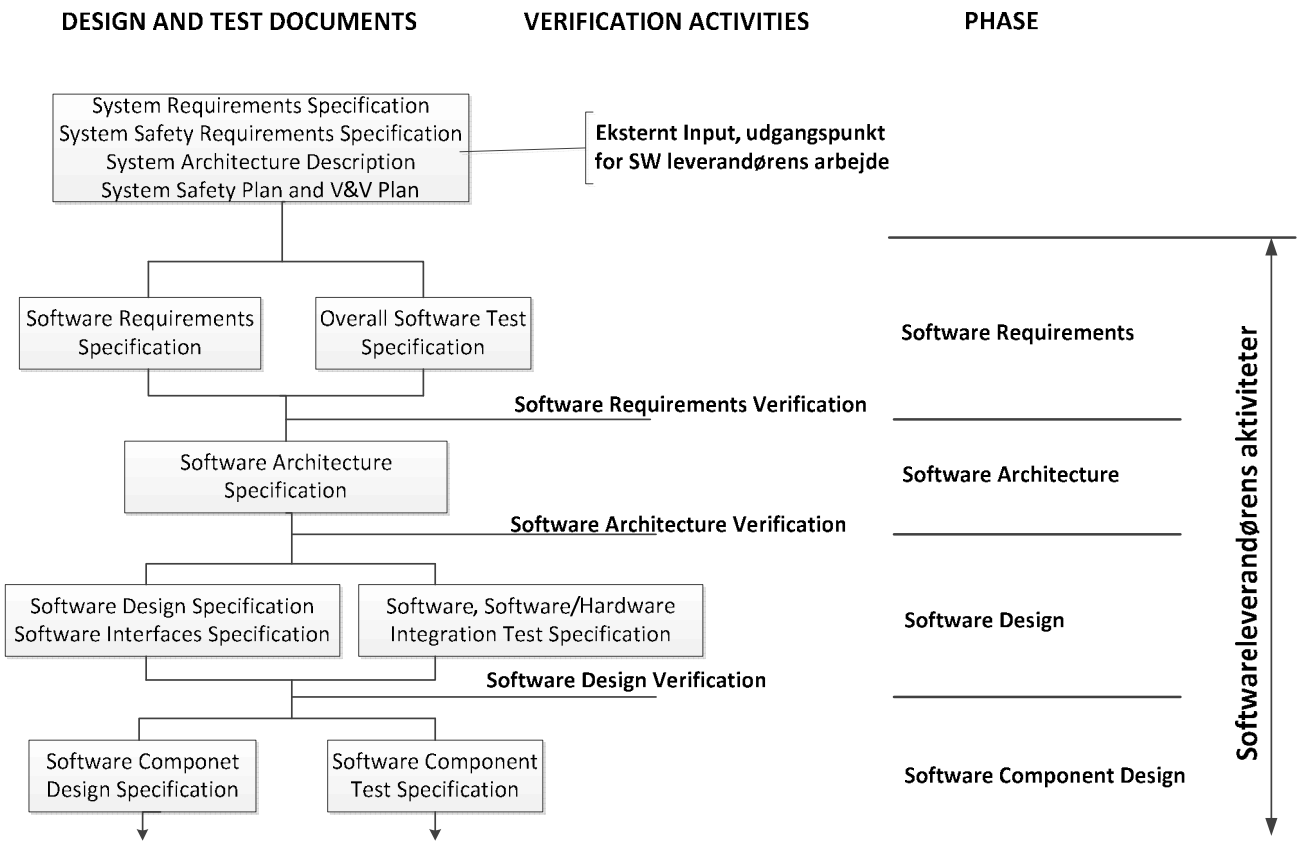
Når CSM sikkerhedskravene (inkl. SIL) og systemarkitekturen er fastlagt, kan det herefter afgøres, hvilke krav der stilles til softwaren.

Sikkerhedskravene til softwaren kan groft opdeles i to dele:

1. Et krav til SW sikkerhedsintegriteten (SSIL).
2. Krav til SW sikkerhedsfunktioner, hvor fabrikanten har formuleret, hvilke sikkerhedsfunktioner SW skal løse.

Ad 1: Bestemmelsen af SSIL tager udgangspunkt i sikkerhedsfunktionens SIL. Afhængig af systemarkitekturen, der er brugt, og om der er brugt flere uafhængige computere / programmer til at løse sikkerhedsfunktioner i SW, kan SSIL i visse tilfælde være lavere end SIL. Anerkendte metoder for dette fremgår bl.a. af EN50129 /6/.

Life Cycle modellen
Den mere detaljerede metode til fastlæggelse af kravene til softwaren fremgår af EN50128, som i bund og grund er opbygget efter den såkaldte "Life Cycle Model". Modellen, vist på Figur 5, er et eksempel på en sådan Life Cycle Model, hvor trinnet mellem fastlæggelsen af CSM sikkerhedskravene og "Software Requirements Phase", er af særlig interesse. Det er her SW leverandørens arbejde starter.



Figur 5 "Udsnit af Life Cycle Model" for SW (ref. figur 3 i EN50128)

Med udgangspunkt i forslagsstillers:
- Systemkravspecifikationen, (brugerkrav, og lovbestemte krav, fx TSI CCS)
- System sikkerhedskravspecifikationen (=CSM sikkerhedskravene),
- En beskrivelse af systemarkitekturen (=CSM systemdefinitionen)
- En sikkerhedsplan,

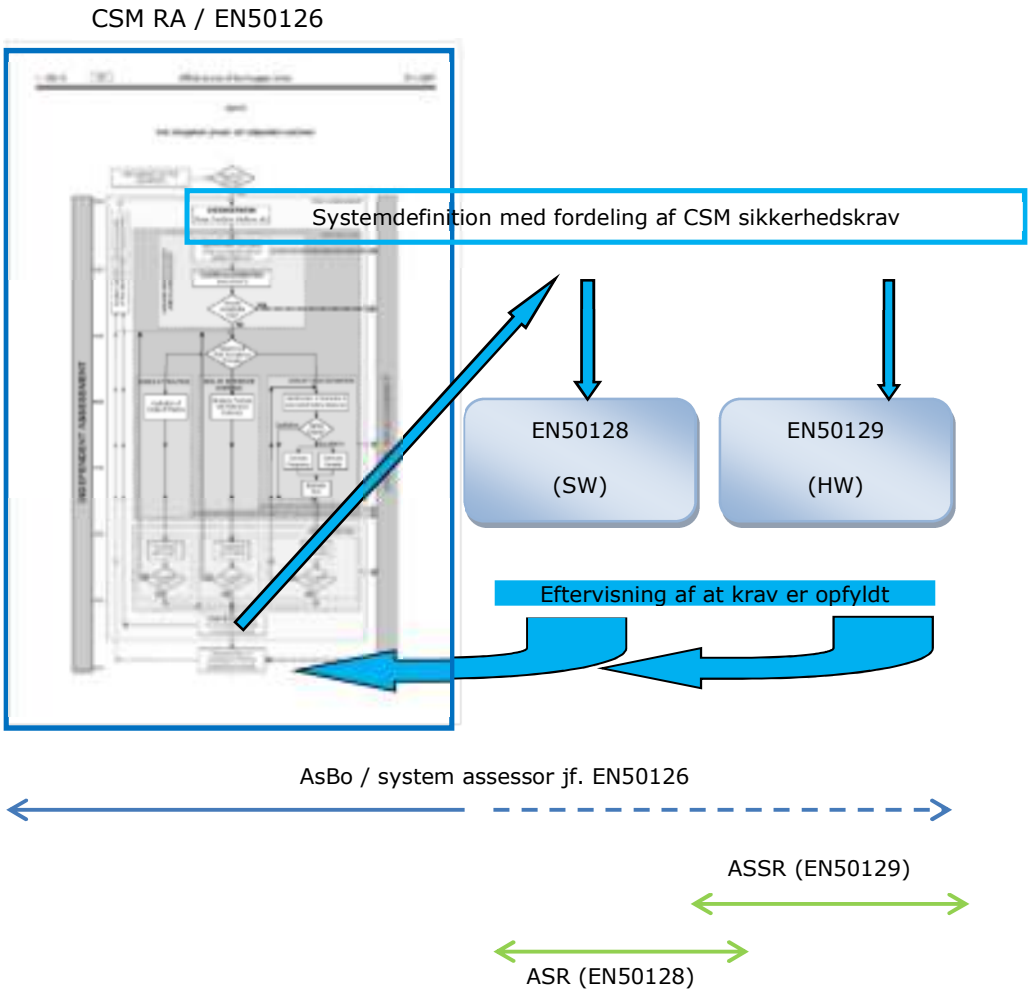
udarbejder SW leverandøren bl.a.:
- Software kvalitetsplan (Software Quality Assurance Plan iht. EN50128)
- Software kravspecifikationen (se definition),
- Software test specifikationen,
- Softwarekravverifikationsrapporten.

I forbindelse med udarbejdelsen af softwaretestspecifikationen, fastlægges det, i hvilken udstrækning SW leverandøren og systemleverandøren skal udføre systemtest.

I nogen tilfælde er det tilstrækkeligt at afprøve softwaren i en testopstilling i et laboratorium. I andre tilfælde er det SW leverandøren, som afprøver softwaren i det endelige delsystem.

Anvendelse af fagassessorer

Nedenstående Figur 6 viser, hvordan sammenhængen er mellem CSM RA og EN standarderne, hvor EN50128 og EN50129 indgår som proces til at vise CSM sikkerhedskravenes opfyldelse og som anerkendt praksis til risikostyring af farer hørende til systematiske fejl.



Figur 6 Sammenhænge mellem CSM RA og EN5012x

Ved fagassessorer forstås assessorer, som er specialister inden for deres respektive område, fx ASR (software assessor jf. EN50128) og ASSR (hardware assessor jf. EN50129). Resultatet af fagassessorernes assessment kan indgå som dokumentation over for AsBo (CSM assessor), for at CSM sikkerhedskravene er opfyldt.

I mange tilfælde vil der også være en rolle som "system assessor" jf. EN50126 og såfremt ændringen er signifikant, kan system assessor og AsBo være én og samme organisation.

I forhold til Figur 6 bemærkes at:

- AsBo er ved signifikante ændringer ansvarlig for assesseringen af det samlede system (HW og SW), men er samtidig afhængig af fagassessorernes arbejde.
- Da SW-validering i nogen tilfælde inkluderer afprøvning med det endelige system, kan ASR assesseringen også omfatter dette. Omvendt kan det være nødvendigt for HW fabrikanten at afprøve systemet med en konkret SW. Derfor kan ASSR assesseringen også omfatte dette[7].

[7] Når en ændring vedrører serier af ens systemer - fx serier af kørertøjer, bør testomfanget, herunder verifikationsomfanget for serien yderligere være fastlagt

- Rollerne som fagassessorer og AsBo kan, når kompetencen er til stede, udgøres af samme organisation.

Som det fremgår af ovenstående, kan det være nødvendigt at re-validere HW funktionaliteten. Det kan med andre ord være nødvendigt at involvere HW leverandøren og dennes assessor, for at re-validere og assessere HW – selv om der kun ændres SW kode. Dette skyldes at SW er en del af CSM-systemet, og hvis SW ændres, ændres samtidigt hele systemet.

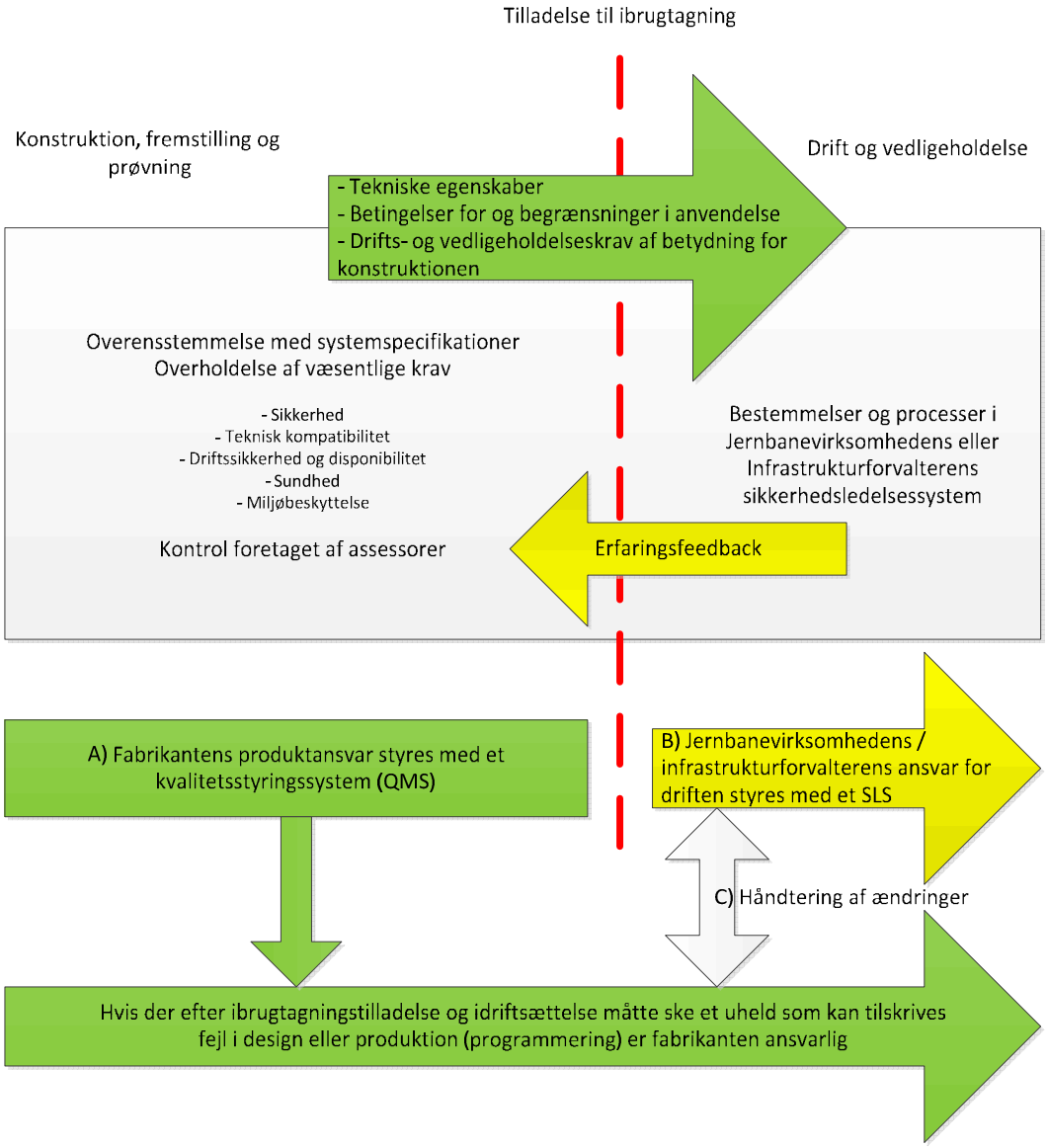
Det følger af EN50128, at det er fabrikanten som, over for ASR dokumenterer, at kravene i EN50128 er opfyldt.
Det følger af CSM RA, at det er forslagsstiller, som over for CSM assessor (AsBo) dokumenterer, at kravene i CSM RA er opfyldt (såfremt ændringen er signifikant).

Der er følgende arbejdsdeling mellem AsBo og ASR:

Enten:
1) AsBo har selv personale til at vurdere overensstemmelse med EN50128, og kan derfor også selv agere ASR. AsBo udarbejder SVR, som har et selvstændigt afsnit for opfyldelsen af EN50128, eller en selvstændig assessment rapport, der vedlægges SVR.
Eller:
2) AsBo forestår ikke selv assesseringen af om kravene i EN50128 er opfyldt. AsBo skal stadig se ASRs rapport, som dokumentation for, at EN50128 er anvendt tilfredsstillende, så sikkerhedskrav herunder SIL kan anses for at være opfyldte. I dette tilfælde bør AsBo sikre sig, at ASR har de rigtige ressourcer og kompetencer samt er uafhængig.

Kravene til ASRs kompetencer og uafhængighed fremgår af EN50128. ASR bør ikke være en del af fabrikantens eller ordregivers organisation, med mindre dette på forhånd er aftalt med Trafik- og Byggestyrelsen.

Roller og ansvar
Nedenstående Figur 7, viser ansvarsfordelingen mellem fabrikanten, som udvikler/ændre SW, og kunden[8], som fx kan være en jernbanevirksomhed.



Figur 7 Ansvarsfordeling mellem fabrikant og jernbanevirksomhed /infrastrukturforvalter

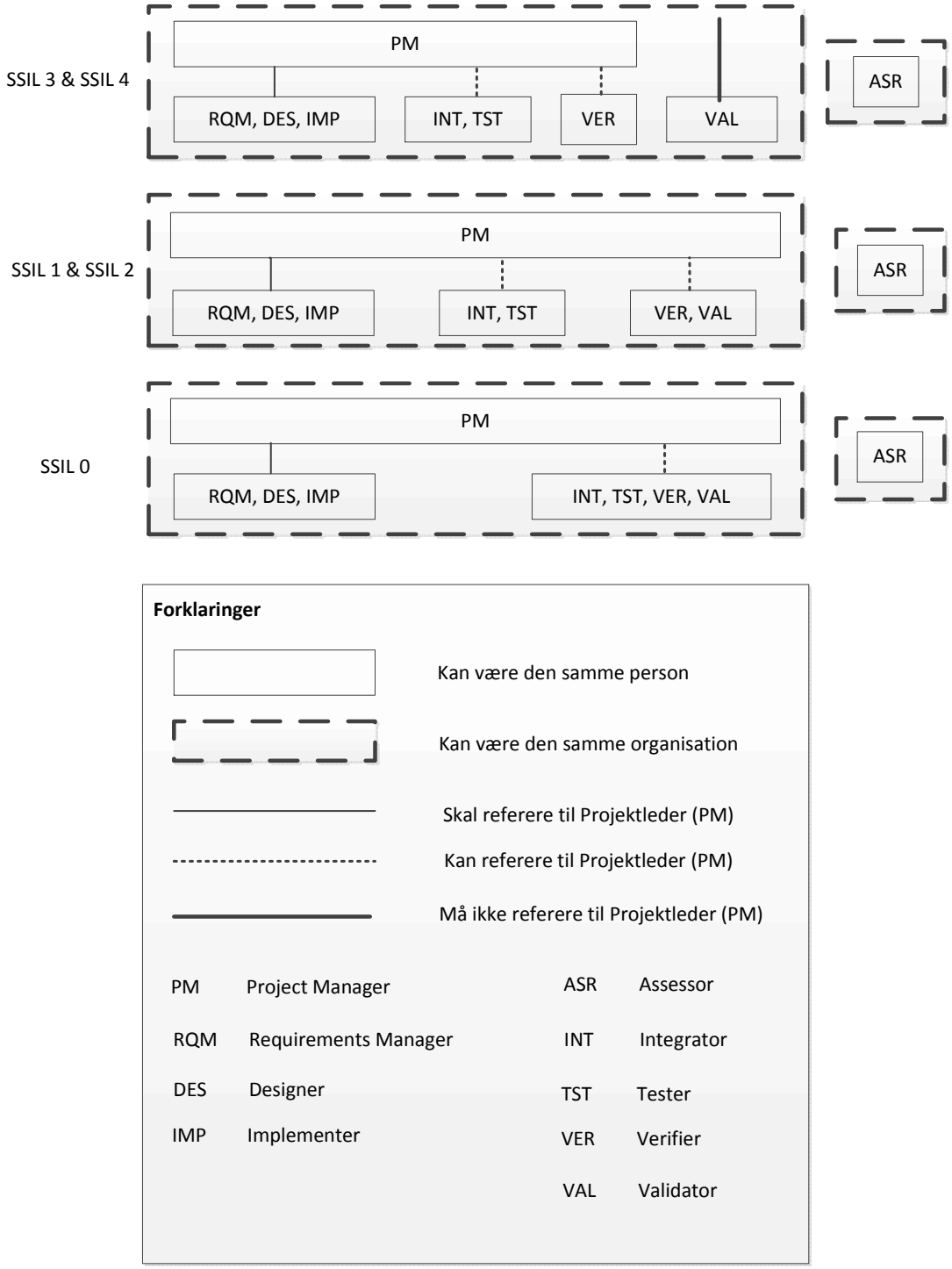
Fabrikantens ansvarsområde jf. A) i Figur 7

I EN50128 (kapitel 5) stilles der krav til fabrikantens kvalitetsstyringssystem. Dette skal som minimum implementere de dele af ISO 9001, som handler om organisation og ansvarsfordeling.

[8] Hvis jernbanevirksomheden eller infrastrukturforvalteren selv forestår udvikling/ændring er denne at betragte som fabrikant.

I standardens bilag B er der desuden defineret en række personalefunktioner og kompetencekrav, som vedrører SW udvikling/ændring. Fabrikantens QMS skal sikre, at det projektteam, som tildeles en SW udviklings- eller ændringsopgave, varetager de roller, der fremgår af EN standarden, og er organiseret i overensstemmelse med standarden.

Nedenstående Figur 8, fra EN50128, viser hvorledes et SW projekt kan være organiseret, i afhængighed af SSIL niveauet. Figuren viser dog ikke alle roller jf. EN50128. Fx er funktionen "configuration manager" ikke vist. Det er selvsagt vigtigt at fabrikantens konfigurationsstyring er veldokumenteret bl.a. af hensyn til overdragelsen af softwaren til kunden (jernbanevirksomheden/infrastrukturforvalteren).



Figur 8 Organisering af SW projekter (ref. figur 2 i EN50128)

Jernbanevirksomhedens/infrastrukturforvalterens ansvarsområde jf. B) i Figur 7.

Jernbanevirksomhedens/Infrastrukturforvalterens primære ansvar er, at det godkendte system anvendes i overensstemmelse med dets anvendelsesbetingelser. Dvs. at det betjenes og vedligeholdes i overensstemmelse med fabrikantens instruktioner.

Jernbanevirksomheder og infrastrukturforvaltere forventes ikke at have kompetencer til at udvikle/ændre SW i overensstemmelse med EN50128 (det er fabrikantens ansvar). Det er derimod nødvendigt at jernbanevirksomheden/infrastrukturforvalteren, via sit sikkerhedsledelsessystem, udpeger det personale, som har kompetencer til - og ansvar for - at håndtere ændringer.

C) Håndtering af ændringer

Når der ændres / fornyes SW, er det vigtigt, at der er et klart overblik over følgende:

- hvor i systemet er ændringen, og hvor omfattende er ændringen,
- hvilke konfigurationer, der findes og hvordan de er konfigurationsstyret, og
- hvad der berøres af ændringen på systemniveau.

Ændringer i SW nødvendiggør en dialog mellem de implicerede parter. Der kan derfor være behov for en dialog mellem RU/IM, NoBo, ASR, AsBo, DeBo, Trafik- og Byggestyrelsen, en køretøjssagkyndig mfl..

I de tilfælde, hvor der er udarbejdet en EF verifikationserklæring, kan det være nødvendigt at denne suppleres (af fabrikanten/ordregiver) i overensstemmelse med Bilag V til interoperabilitetsdirektivet. Dette kan medføre, at det tekniske dossier, som ledsager EF verifikationserklæringen, skal opdateres.

Jernbanevirksomheden/infrastrukturforvalteren skal inden ibrugtagning via sit sikkerhedsledelsessystem sikre sig, at ændringen er blevet vurderet af kompetente parter således:

i. SW ændringens kritikalitet bør vurderes af fabrikanten.
ii. Om en ændring skal betragtes som fornyelse/opgradering jf. interoperabilitetsdirektivet, skal vurderes af ordregiver eller fabrikanten.
iii. Om allerede udstedte verifikationsattester påvirkes af ændringen, skal vurderes af NoBo/DeBo/køretøjssagkyndige.
iv. Om ændringen er signifikant, jf. CSM RA, skal vurderes af forslagsstiller.

Ad i.: Når der er behov for ændring af SW, forskriver standarden EN50128, afsnit 9.2.4.2, at fabrikanten indledningsvis vurderer om en ændring skal betragtes som "major" (i så fald anvendes standarden fuldt ud) eller "minor" (i så fald anvendes afsnit 9.2 om vedligehold af SW).

Imidlertid fremgår det ikke af standarden, hvad der skal forstås ved 'minor' og 'major'. Bilag 1 beskriver derfor en procedure, som kan anvendes til fastlægning af, om der er tale om en minor eller major ændring. I henhold til EN50128, afsnit 1.9, skal vurderingen af ændringens kritikalitet (major/minor) forelægges en ASR.

Ad ii.: Ordregiver vil typisk være en jernbanevirksomhed eller en infrastrukturforvalter.

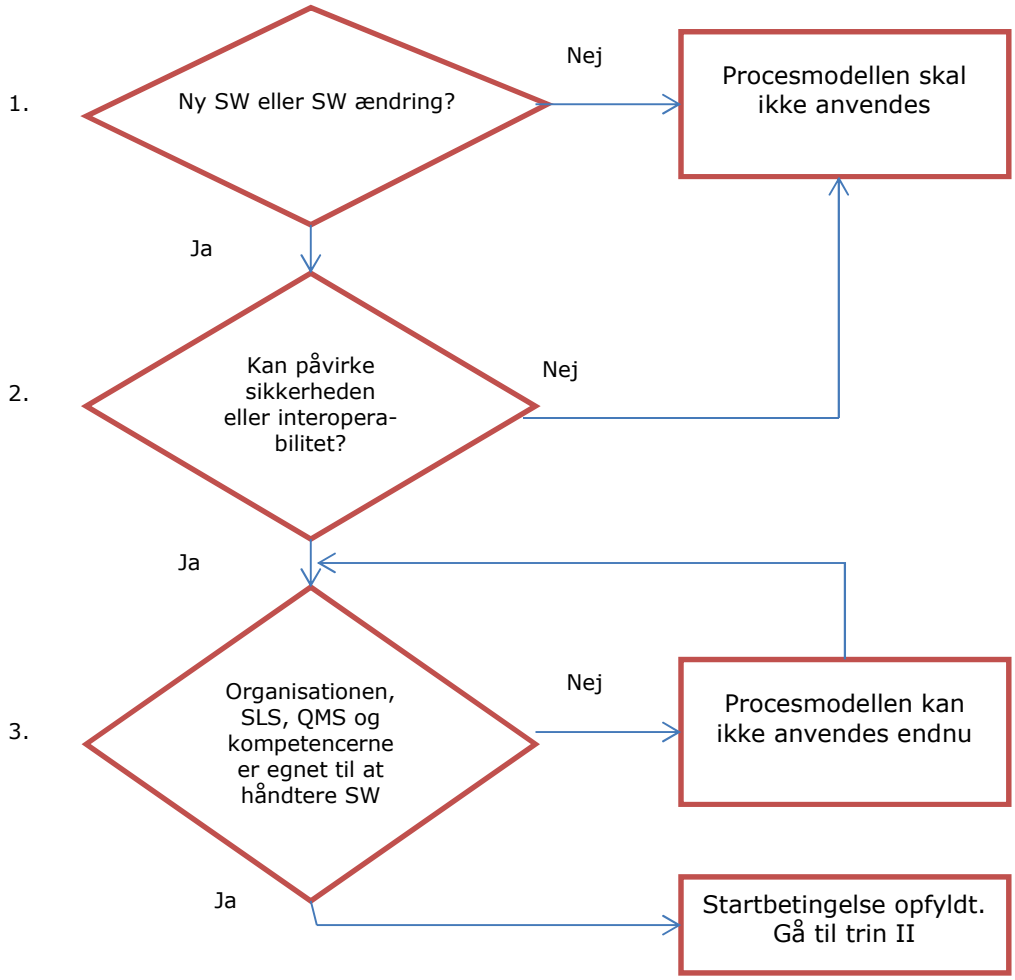
Ad iii.: Såfremt der foretages ændringer, der kan påvirke allerede udstedte verifikationsattester, skal ændringen forelægges den NoBo/DeBo/køretøjssagkyndige som har udarbejdet verifikationsattesten med henblik på en vurdering af attestens fortsatte gyldighed.

Ad iv.: Se evt. kapitel 5 vedr. hvem der kan være forslagsstiller. Det er vigtigt, at det fra starten aftales, hvem der skal være forslagsstiller i projektet. Da CSM processen i sidste ende skal sikre at jernbanesystemets delsystemer integreres sikkert, vil det ofte være naturligt, at infrastrukturforvalteren eller jernbanevirksomheden agerer forslagsstiller. Navnlig hvis der er tale om ændringer på "railway level" dvs. ændringer i den måde delsystemerne interagerer på.

Processen for ændringsvurdering er nærmere beskrevet i de følgende afsnit.

8. Procesmodellen (I) – Startbetingelser

I det efterfølgende kapitel er vist en procesmodel, som kan anvendes til at bestemme om et givent system med SW, skal forelægges Trafik- og Byggestyrelsen. Før procesmodellen anvendes er det vigtigt at følgende startbetingelser er undersøgt:



Figur 9 Startbetingelser

Ad 1: Forslagsstiller har undersøgt og konstateret, at det drejer sig om en softwareændring[9] i jernbanesystemet. Det kan fx være ændring af programmet eller data.

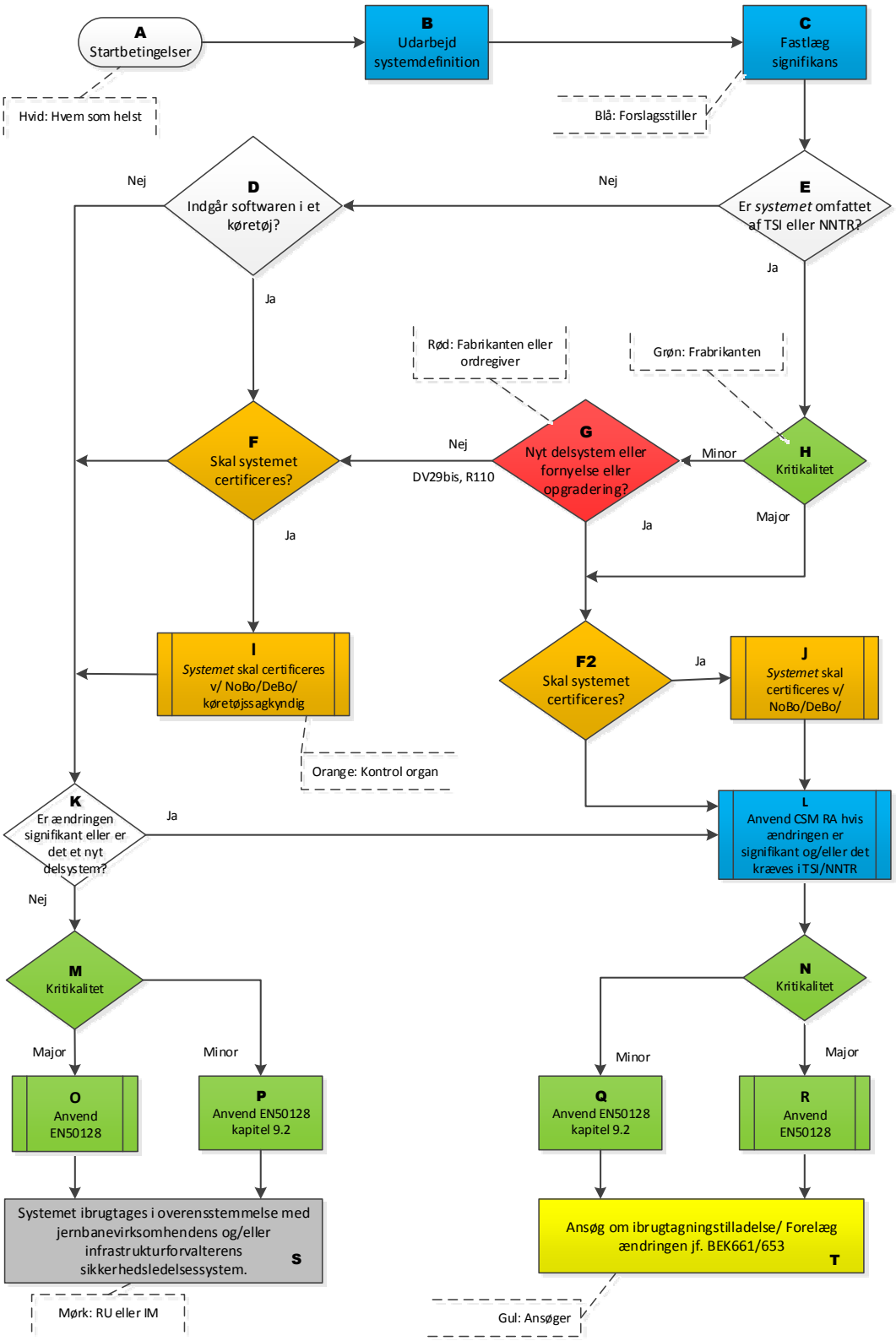
Ad 2: Ligeledes har forslagsstiller konstateret, om softwaren har indflydelse på sikkerheden[10], hvilket vil sige, at SW og fejl i SW i værst tænkelige tilfælde kan medføre en eller anden form for ulykke. Hvis interoperabilitet kan påvirkes, skal der også svares 'ja'.

Ad 3: Indførelsen af det nye system eller ændringen af det eksisterende sker ved anvendelse af et SLS / QMS, og der er indført procedurer for håndtering af SW, herunder konfigurationsstyring. Det er samtidig konstateret at rette kompetencer til at forestå processen er til stede.

[9] Fejlretning af SW skal også betragtes som en ændring. Mere herom i kapitel 13.

[10] Forslagsstiller skal opbevare dokumentation for sin vurdering uanset om det vurderes at ændringen påvirker sikkerheden eller ej. Trafik- og Byggestyrelsen kan føre tilsyn hermed.

9. Procesmodellen (II) – Flowdiagram



Forklaringer til procesmodellen

Box	Forklaring
A	**Startbetingelser** Se kapitel 8 ang. forudsætninger for processen. Betydningen af de anvendte kasser er:  = en proces eller aktivitet,  = en beslutning,  =information om at der findes en underproces. Kassernes farver viser hvem, som skal forestå processen/aktiviteten/beslutningen. Farverne er forklaret på figuren.
B	**Systemdefinition for systemer med SW** Den foreløbige systemdefinition skal udformes, så den understøtter vurderingen af signifikans. Se kapitel 10.
C	**Fastlæg om ændringen er signifikant** Om ændringen er signifikant, skal afgøres af forslagsstiller og her henvises til kapitel 13. Forslagsstiller kan være RU, IM eller ECM inden for rammerne af vedligehold af systemet eller en som ansøger om ibrugtagningstilladelse.
D	**Indgår softwaren i et køretøj?** Der vælges "ja" hvis softwaren indgår i et system i et køretøj.
E	Systemer, som er omfattet af interoperabilitetsdirektivet, kan være omfattet af TSI eller NNTR krav: Interoperabilitetsdirektivet (2008/57/EF) omfatter hele det danske jernbanenet og køretøjer som befarer dette, undtagen følgende jernbanesystemer, som er undtaget i medfør af bekendtgørelse nr. 1281 af 19. november 2015 om interoperabilitet i jenbanesystemet: a) Metro, sporvogne og andre letbanesystemer. b) S-banenettet og køretøjer der udelukkende anvendes her. c) Privatejet jernbaneinfrastruktur og køretøjer, der udelukkende bruges på denne infrastruktur til ejerens egen godstransport. d) Infrastruktur der udelukkende anvendes til lokale, historiske eller turistmæssige formål, og køretøjer der udelukkende kører på denne infrastruktur. Der vælges "nej", såfremt der er tale om et system, der er undtaget. Se kapitel 11 ang. TSI krav.
F	**Skal systemet med SW certificeres?** Der vælges "ja" i følgende tilfælde: 1) Nyt køretøj, som ikke er omfattet af IOD. 2) Ændret delsystem, som er omfattet af en verifikations- eller typeafprøvningsattest, der mister sin gyldighed pga. ændringen. Se desuden kapitel 12 for mere vejledning om certificering af systemer med SW.
F2	**Skal systemet certificeres?** Der vælges "ja" i følgende tilfælde: 1) Nyt delsystem. 2) Ændret delsystem, som er omfattet af en verifikations- eller typeafprøvningsattest, der mister sin gyldighed pga. ændringen. Se desuden kapitel 12 for mere vejledning om certificering af systemer med SW.
G	**Nyt delsystem eller fornyelse eller opgradering**

	Er det et nyt delsystem, er svaret altid 'ja'. Fornyelse og opgradering er defineret i Interoperabilitetsdirektivets artikel 2: m) »opgradering«: større arbejder, som går ud på at ændre et delsystem eller en del af et delsystem, og som forbedrer delsystemets samlede ydeevne, n) »fornyelse«: større arbejder, som går ud på at udskifte et delsystem eller en del af et delsystem uden at ændre delsystemets samlede ydeevne. Yderligere vejledning gives i kapitel 11, og i Kommissionens henstilling (2014/897/EU), anbefaling nr. 110.
H, M, N	**Kritikalitet** Kritikaliteten (dvs. om ændringen er major eller minor jf. EN50128) skal bestemmes af fabrikanten og er afgørende for, i hvilken udstrækning EN50128 skal anvendes. I bilag 1 gives vejledning, om hvorledes kritikaliteten kan bestemmes. Beslutningen om minor/major skal være accepteret af ASR jf. EN50128.
I, J	**Systemet med SW skal certificeres v/ NoBo/DeBo/køretøjssagkyndig** I de tilfælde hvor systemet med SW skal certificeres bør softwarens baseline fremgå af attesterne. Det anbefales også at fastlægge såkaldte "forudbestemte varianter", som gør det muligt senere at ændre systemet, inden for fastlagte rammer, uden at der skal udstedes nye attester. Se kapitel 12.
K	**Er ændringen signifikant eller er det et nyt delsystem** Se C og kapitel 13 vedr. signifikansvurderingen. Er der tale om et nyt delsystem, skal der altid vælges "ja".
L	**Anvendelse af CSM RA** Såfremt ændringen er signifikant, anvendes CSM RA til styring af den sikre integration, og AsBo skal udarbejde en sikkerhedsvurderingsrapport. Såfremt CSM RA skal anvendes til bestemte formål, specificeret i en TSI/NNTR, anvendes metoden til dette formål.
O, R	EN50128 anvendes fuldt ud, og ASR skal udarbejdet en assessmentrapport.
P, Q	For ændringer, der kategoriseres som "minor", er det kun EN50128 standardens kapitel 9.2 som finder anvendelse. Dette betyder, at ændringen bør styres i overensstemmelse med DS/ISO/IEC 90003:2015, Softwareudvikling – Retningslinjer for anvendelse af ISO 9001:2008 til computersoftware.
S	Jernbanevirksomheden/infrastrukturforvalterens SLS bør indeholde procedurer for hvorledes systemer med SW skal håndteres. Trafik- og Byggestyrelsen kan føre tilsyn hermed. Følgende dokumentation bør kunne fremvises: • Signifikansvurdering og foreløbig systemdefinition, • ASRs assessering af kritikalitetsbestemmelsen, i tilfælde af en "minor" ændring, • ASRs assessment rapport i tilfælde af 'major' ændringer.
T	Se kapitel 14 ang. indholdet i sikkerhedsvurderingsrapporten, ændringsforelæggelse mm.

10. Systemdefinitionen for systemer med SW

Trafik- og Byggestyrelsens generelle vejledning om udformning af systemdefinitioner, finder også anvendelse for de systemer, hvori der indgår SW. Imidlertid er der i forbindelse med systemdefinitionen for systemer, hvor SW indgår, brug for en vægtning af oplysninger rettet mod netop SW, hvilket er målet med dette kapitel. Såfremt særlige egenskaber kun kan illustreres ved SW arkitekturen eller designet findes i Bilag 1 yderligere vejledning hertil.

Systemdefinitionens opbygning
Systemet med SW defineres med udgangspunkt i CSM-Systemet og dets grænseflader. Se Figur 3.

Nedenstående understregede overskrifter er fra vejledningen om systemdefinitioner, og for hver overskrift er der anført supplerende emner med relevans for systemer med SW.

For ændringer er det vigtigt at beskrive både nu situationen og den ønskede nye situation.

a. en systemmålsætning, f.eks. det tilsigtede formål

Årsag til ændring fx ønsket om nye funktioner, fejlretning, ny SW platform, ny HW, osv.

b. systemfunktioner og –elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationelle elementer)

Overordnet skal det skitseres i et blokdiagram, hvor i det overordnede system/delsystem computeren / computerne befinder sig (Se eventuelt Figur 12).

Ændringer i implementeringen af systemfunktioner beskrives og det vises hvilke sikkerhedsfunktioner der løses af SW og hvilke der fx løses mekanisk; Elektrisk; Pneumatisk; Fysisk; Instruktorisk.

Eventuelle nye funktioner beskrives.

Eventuelle nye SIL-klassifikationer pga. ændringer i implementeringen og systemarkitekturen angives.

c. systemafgrænsning, herunder vekselvirkninger med andre systemer

Tegning evt. med anvendelse af forskellige farver eller figurer, der viser afgrænsningen. Beskrivelse af hvordan computeren / computerne indgår i CSM- og delsystemets funktioner.

d. fysiske (dvs. vekselvirkende systemer) og funktionelle (dvs. funktionelt input og output) grænseflader

Et af de vigtigste kapitler i systemdefinitionen, der lettest beskrives med en tegning. Tegningen bør vise de indre og ydre grænseflader.

Følgende bør vises

- Grænsefladen fra computerens Input/Output til andre elementer i CSM-systemet
- Fælles grænseflader fx til en fælles BUS
- Er der flere computere, vises hvor grænsefladen er til disse
- Grænsefladen mellem CSM-systemet og delsystemet vises
- Grænsefladen mellem delsystemet og nabosystemer vises

e. systemmiljøet (f.eks. energi- og varmestrømme, stød, vibrationer, elektromagnetisk interferens, operationel anvendelse)

Her beskrives det systemmiljø som CSM-systemet og computeren skal arbejde i.

f. eksisterende sikkerhedsforanstaltninger og, efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen

Udgangspunktet for softwareudviklingen/ændringen beskrives, dvs.:

- CSM sikkerhedskravene inkl. SIL.

Bemærk at software kravspecifikationen, herunder SSIL, ikke nødvendigvis behøver at indgå i CSM systemdefinitionen, da dette ikke behøver at høre til CSM risikovurderingen. Se Figur 4, Figur 5 og Figur 6.

SW udviklingen/realiseringen af en ændring, kan føre til at CSM sikkerhedskravene, og systemdefinition, skal ændres. Dette sker i en iterativ udviklingsproces. Hvis der identificeres nye CSM sikkerhedskrav i forbindelse hermed, skal disse nye krav fremgå af systemdefinitionen. I den forbindelse kan der også opstå et behov for at ændre beskrivelsen i andre af systemdefinitionens afsnit.

g. antagelser med henblik på at afgrænse risikovurderingen

Her kan fx anføres forskellige antagelser og forudsætninger om udviklings-, verifikations- og valideringsprocesser, der anvendes ved ændringen af SW som fx:

- Programmeringsmiljø (inklusiv procesflow fra kode til compiler, linker, eksekverbar fil og installering)
- Anvendelse af anerkendte maskinelle valideringsmetoder
- Anvendelsen af testfaciliteter – testlaboratorier og om de er certificerede
- Ændringslog og versionsstyringssystemer
- Organisation og kompetencer hos de involverede
- Om fabrikantens kvalitetsstyringssystem er certificeret til at udvikle SW

11. Fornyelse eller opgradering

Når et delsystem, som er omfattet af interoperabilitetsdirektivet, ændres, skal det afgøres, om der er tale om fornyelse eller opgradering. Formålet hermed er at sikre, at delsystemet forbliver interoperabelt, hhv. bevæger sig i en retning, så det ender med at være interoperabelt.

Delsystemer som er bygget i overensstemmelse med NNTR og TSI krav, er pr. definition interoperable. NNTR og TSIerne definerer med andre ord det tilstrækkelige og nødvendige niveau af interoperabilitet. Det er således også NNTR og TSIernes krav, der skal lægges til grund for vurderingen af om en given ændring skal betragtes som en opgradering eller fornyelse. I nedenstående tabel gives eksempler på bestemmelser i TSI´erne som relaterer sig til SW:

TSI	**KRAV**	**BEMÆRKNING**
LOC&PAS:2014, afsnit 4.2.1.3	*4) Elektronisk udstyr og software, der bruges til at varetage sikkerhedskritiske funktioner, skal udvikles og vurderes efter en metode, der egner sig til sikkerhedsrelateret elektronisk udstyr og software.*	Det er ikke obligatorisk at anvende EN50128/EN50129, til demonstration af overensstemmelse med 4.2.1.3, men det kan anses som anerkendt praksis, hvis man gør det.
TSI CCS 2012/88/EU, med senere ændringer, tabel 6.1, aspekt: *Pålidelighed, tilgængelighed, vedligehold og sikkerhed (RAMS)*	*Kontrollér, at sikkerhedskravene som specificeret i de grundparametre, der er henvist til i den relevante tabel i kapitel 5, er opfyldt, dvs.:* *1. De kvantitative acceptable farehyppigheder, der skyldes tilfældige svigt, skal overholdes.* *2. Udviklingsprocessen skal kunne opdage og eliminere systematiske svigt.*	Det er obligatorisk at anvende EN50126/EN50128/EN50129 til demonstration af overensstemmelse med RAMS krav, på komponent niveau. Det er valgfrit, om version 2001, eller version 2011 af EN50128 anvendes.
…		

Tabel 1: Eksempler på SW relaterede krav i TSIer

I de tilfælde hvor der stilles krav om at SW udvikles efter egnede metoder, fx kravet i TSI LOC&PAS:2014, afsnit 4.2.1.3, bør ændringer, der klassificeres som ”major” jf. bilag 1 i denne vejledning også betragtes som ”fornyelse eller opgradering”.

12. Certificering af systemet med SW

Nedenstående afsnit tager udgangspunkt i at CSM-systemet indgår i delsystemet, der er omfattet af krav i NNTR eller TSI´er, men principperne gælder også for køretøjer der certificeres af en køretøjssagkyndig.

Det er nødvendigt at inddrage et NoBo/DeBo, når:

1) Der er tale om et nyt delsystem, som er omfattet af en NNTR/TSI, fx CCS onboard eller CCS trackside,
2) Der er tale om en ændring i et delsystem, som er omfattet af allerede udstedte verifikationsattester, herunder ændringer i anvendte interoperabilitetskomponenter,
3) Trafik- og Byggestyrelsen, i tilfælde af fornyelse eller opgradering, afgør at TSI/NNTR krav finder anvendelse.

I ovenstående tilfælde 1) udarbejder NoBo/DeBo en verifikationsattest, hvori overensstemmelsen med relevante TSI/NNTR krav fastholdes. Alt efter hvilket verifikationsmodul[11] der er valgt, udarbejdes der ligeledes en typeafprøvningsattest (modul SB) eller en konstruktionsundersøgelsesattest (modul SH).

Såfremt der foretages ændringer i et allerede certificeret delsystem (tilfælde 2) ovenfor), skal reglerne i modulbeskrivelserne følges. I modul SB står bl.a.

”8. Ansøgeren underretter det bemyndigede organ, der opbevarer den tekniske dokumentation for EF-typeafprøvningsattesten, om alle ændringer af den godkendte type, som kan påvirke delsystemets overensstemmelse med kravene i den eller de relevante TSI'er eller betingelserne for attestens gyldighed. Sådanne ændringer kræver en tillægsgodkendelse i form af en tilføjelse til den oprindelige EF-typeafprøvningsattest.

9. Hvert bemyndiget organ orienterer sine bemyndigende myndigheder om udstedte eller tilbagekaldte EF-typeafprøvningsattester og/eller tillæg hertil og stiller med jævne mellemrum eller efter anmodning en fortegnelse over afviste, suspenderede eller på anden måde begrænsede attester og/eller eventuelle tillæg hertil til rådighed for sine bemyndigende myndigheder.

Hvert bemyndiget organ oplyser de øvrige bemyndigede organer om de EF-typeafprøvningsattester og/eller tillæg hertil, som det har afvist, trukket tilbage, suspenderet eller på anden måde begrænset, og, efter anmodning, om de attester og/eller tillæg hertil, som det har udstedt.”

Når en typeafprøvnings- eller konstruktionsundersøgelsesattest udarbejdes bør der i denne specificeres, hvilken SW baseline der indgår i computerne. Hvis der foretages ændringer, som kan påvirke attestens gyldighed, er man forpligtiget til at underrette NoBo/DeBo/køretøjssagkyndige, således at denne har mulighed for at vurdere attestens fortsatte gyldighed og evt. udarbejde et tillæg eller en ny attest.

For at minimerer behovet for at få udstedt nye attester kan attesterne omfatte ”forudsete varianter”. En forudset variant kan fx gøre det muligt at ændre i bestemte tabeller i SW, uden at attesterne derved mister deres gyldighed.

[11] Verifikationsmodulerne er beskrevet i /12/.

13. Bestemmelse af signifikans

Trafik- og Byggestyrelsens generelle vejledning om signifikansvurdering finder også anvendelse på systemer, hvori der indgår SW. Da SW har mangfoldige egenskaber, vil det være nødvendigt at supplere visse kriterier, og i visse tilfælde vil det være overflødigt at foretage en signifikansvurdering.

Ændringer, der kan betragtes som ikke signifikante

SW ændringer, som ikke har nogen påvirkninger på CSM sikkerhedskravene, kan betragtes som ikke signifikante. Dette kan siges at være tilfældet, såfremt følgende betingelser alle overholdes:

1. Systemdefinitionen er uforandret.
2. SW, der ændres, er i drift.
3. CSM RA eller EN50126 har været anvendt til at opstille sikkerhedskrav til systemet, og SW er udviklet efter EN50128 og er blevet vurderet af ASR.
4. Ændringen vil følge EN50128 og blive vurderet på ny af ASR.
5. 1-4 skal begrundes og være accepteret af den assessororganisation, der har udarbejdet sikkerhedsvurderingsrapporten for systemet.

Ad 1.

Hvis der ikke sker ændringer i systemdefinitionen (kapitel 10, pkt. a-g), vil systemsikkerhedskravene, og dermed udgangspunktet for at anvende EN50128 være uændret[12]. I dette tilfælde påvirkes risikovurderingen på systemniveau ikke af den tiltænkte ændring (der foretages således ikke ændringer i det eksterne input, som er udgangspunkt for SW leverandøres arbejde, jf. Figur 5).

Alle ændringer siden seneste ibrugtagningstilladelse skal tages i betragtning, fx ændringer i HW.

Selv om der kun foretages SW ændring(er), skal det vurderes om den eksisterende HW validering bliver påvirket. I så fald skal der også foretages en fornyet HW validering og assessering (ved HW fagassessor).

Udviklingen af SW ændringen (fx en fejlrettelse) kan føre til at systemdefinitionen skal ændres, og at risikovurderingen på systemniveau skal genovervejes. I så fald skal ændringen signifikansvurderes for at afgøre, om CSM RA i øvrigt skal følges. Dette gælder uanset om sikkerhedskravene, på systemniveau, i sidste ende bliver ændret eller ej.

Ad 2.

Betingelsen skyldes, at muligheden for at foretage SW ændringer på systemer, der er certificerede og/eller godkendte, men ikke idriftsatte ønskes begrænset bl.a. for at undgå "slicing".

Ad 3 og 4.

At CSM RA / EN50126 har været anvendt til at opstille sikkerhedskrav til systemet, medfører at der allerede foreligger en assesseret systemdefinition med sikkerhedskrav, som der kan tages udgangspunkt i, når ændringen skal udvikles. Når EN50128 tilmed er anvendt, foreligger der ligeledes en SW kravspecifikation, testplan, mm. Dette giver en formodning om, at den eksisterende SW er beskrevet på et niveau, som gør det muligt at lave en SW ændring, som ikke medfører utilsigtede afsmitninger på SW og dermed utilsigtede ændringer af sikkerhedsfunktionerne.

Betingelse 4 giver derudover en sikkerhed for, at der igen vil blive anvendt en metode (EN50128), som netop tager udgangspunkt i CSM sikkerhedskravene, og at den ændrede SW ikke medfører utilsigtede afsmitninger på SW og dermed utilsigtede ændringer af sikkerhedsfunktionerne.Ad 5.

Fordi 1. - 4. indeholder mulighed for utilsigtede tolkninger, er der yderligere den betingelse, at en uafhængig - i forhold til forslagsstiller - er enig i, at betingelserne er opfyldt. Assessors vurdering skal kunne forevises ved tilsyn.

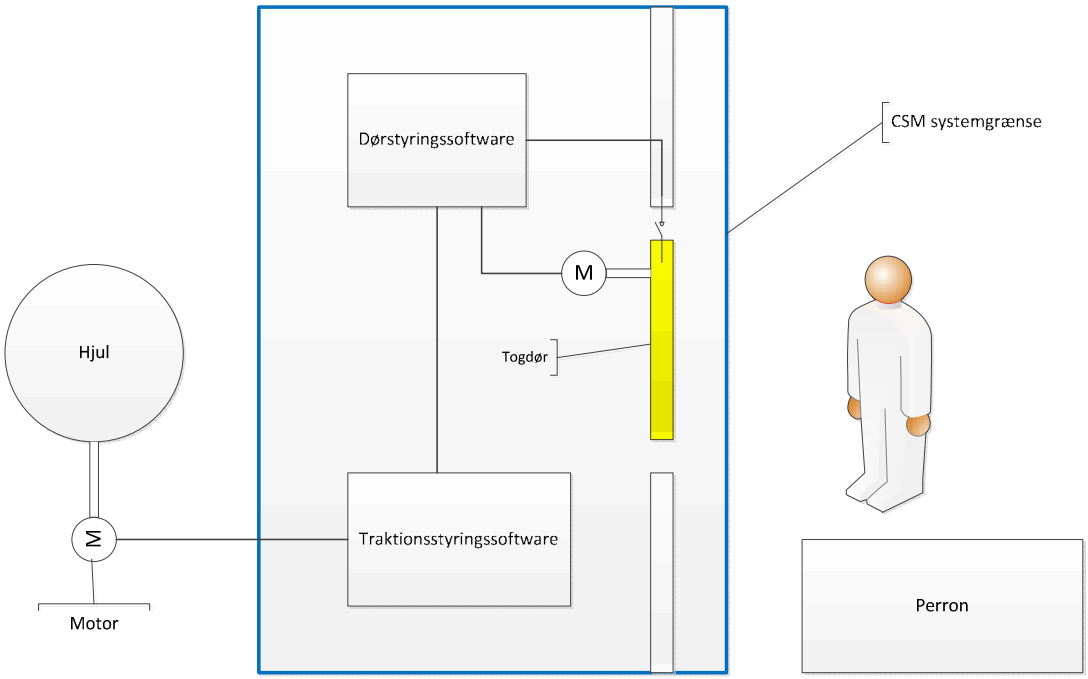
Eksempel på en ændring, der kan betragtes som ikke signifikant:

[12] Trinnet mellem "System Development Phase" og "Software Requirements Phase", er forklaret i kapitel 7, og vist i Figur 5 "Udsnit af Life Cycle Model" for SW.

Dørsystemet, vist i nedenstående Figur 10, er analyseret vha. CSM RA. Analysen har ført til, at der bl.a. er opstillet følgende CSM sikkerhedskrav:

a) Toget må ikke kunne køre, hvis dørene ikke er lukket.

b) Dørene må ikke kunne lukke, hvis der er genstande i døråbningen.



Figur 10 Dørstyringssystem

Sikkerhedskravene implementeres ved hjælp af en kombination af HW og SW. SW sikkerhedsfunktionen udgøres af SW i dørstyringsenheden, og traktionsstyringen i tog computeren. Programmerne er lavet iht. EN50128 af 2 forskellige leverandører. Der foreligger en AsBo sikkerhedsvurderingsrapport, som refererer til 2 ASR rapporter for softwaren og en ASSR rapport for HW.

Efter et stykke tid i drift opstår et ønske om at ændre i dørstyringssoftwaren, da det har vist sig at kommunikationen mellem dørstyring og traktionsstyring er meget langsom. Det er først muligt at sætte i gang 45 sekunder efter at døren er lukket.

Da den ønskede SW ændring kun har til formål at løse et SW internt timings problem, og der ikke er registreret sikkerhedskrav til timing, forventes det, at ændringen ikke vil påvirke CSM sikkerhedskravene. Det ønskes derfor undersøgt om ændringen kan betragtes som ikke signifikant:

Ad 1. Systemdefinitionen

Den oprindelige systemdefinition indeholder i dette eksempel ikke noget sikkerhedskrav, der vedrører tid og timing, så traktion kan, som udgangspunkt godt aktiveres lige efter dørene er lukkede.

Følgende dokumentation udarbejdes:

- Dokumentation/argumentation for at systemdefinition og CSM sikkerhedskrav er uforandrede. Bemærk, at dokumentationen først kan gøres færdig, når softwaren er ændret. Dette skyldes, at der i udviklingsforløbet kan opstå behov for at ændre i SW arkitekturen, som nødvendiggør ændring i CSM sikkerhedskravene, herunder formulering af nye CSM krav, hvorved systemdefinitionen ikke er uforandret.

I eksemplet foretages der ingen HW ændringer. Det kan dog være nødvendigt at inddrage en HW fagassessor, hvis systemvalideringen kræver det. Da dørenes mekaniske funktion og hjulenes slip/slide ikke påvirkes i dette eksempel, vil det ikke være nødvendigt ud fra et sikkerhedssynspunkt.

Ad 2 og 3.

I eksemplet er betingelse 2 og 3 overholdt.

Ad 4 og 5. Ændringen vil følge EN50128 og blive vurderet på ny af ASR.

Følgende dokumenteres:

- Kritikalitetsanalysen (fabrikantens vurdering af om ændringen er major eller minor)
- ASRs assessment af kritikalitetsanalysen.
- ASRs assessment rapport i tilfælde af 'major' ændringer.
- Systemassessorens/AsBo´s vurdering af at betingelse 1-4 er opfyldt.

Fejlretning[13]

Hvis der konstateres fejl i et system med SW efter idriftsættelsen, kan det være nødvendigt at ændre i softwaren for at fjerne fejlen. En fejlretning skal behandles som alle andre typer af ændringer. Dog vil fejlretninger, oftere end andre typer af ændringer, kunne klassificeres som ikke signifikante, jf. betingelse 1-5 ovenfor. Dette skyldes, at der ved fejlretning normalt ikke er nogen intention om at ændre i CSM-systemet eller CSM sikkerhedskravene.

Supplement til signifikanskriterier for systemer med SW

Nedenstående tekst er et supplement til Trafik- og Byggestyrelsens vejledning om signifikansvurering, og forholder sig derfor ikke til HW ændringer.

a) Konsekvens af svigt (et plausibelt, værst tænkeligt scenario i tilfælde af svigt i det system, der er under vurdering, under hensyn til sikkerhedsbarrierer uden for systemet)

Når SW ændringens kritikalitet er major[14], er der som regel tale om en ændring med høj konsekvens ved svigt og således ofte også en signifikant ændring. Se bilag 1.

Ændringens kritikalitet bør (i overensstemmelse med EN50128) afgøres af fabrikanten og vurderes af ASR.

b) Nyskabelse (der anvendes til at gennemføre ændringen: dette gælder både for det, der er innovativt for jernbanesektoren, og det, som alene er nyt for den organisation, der gennemfører ændringen)

Såfremt forslagsstiller kan dokumentere

- at samme organisation har foretaget ændringer før i den pågældende SW
- at den pågældende SW er udviklet efter EN50128 og i drift,
- at SW ændringen vil blive foretaget efter EN50128,
- at der ikke introduceres "innovative" ændringer/funktioner i CSM-systemet,

er der normalt ikke tale om nyskabelse.

c) Ændringens kompleksitet

[13] I EN50128 findes følgende definitioner:

3.1.9 Error, fault: defect, mistake or inaccuracy which could result in failure or in a deviation from the intended performance or behavior.

3.1.10 Failure: unacceptable difference between required and observed performance.

[14]I nogle tilfælde, er der ikke behov for at ændre systemdefinitionen, selv om der er tale om en major ændring. Men AsBo skal alligevel se påvisningen af, at CSM sikkerhedskravene er opfyldte, med mindre ændringen ikke er signifikant.

Når SW ændringens kritikalitet er 'minor' er der som regel ikke tale om en kompleks ændring. Se bilag 1.

Ændringens kritikalitet bør (i overensstemmelse med EN50128) afgøres af fabrikanten og vurderes af ASR.

d) Overvågning (manglende evne til at kontrolovervåge den gennemførte ændring i systemets samlede livscyklus og foretage hensigtsmæssige indgreb)

Såfremt der allerede findes uafhængige tekniske barrierer, som sikrer, at fejl i CSM-systemet opdages med det samme, og der kan gribes ind før der sker ulykker, vil overvågningskriteriet kunne medregnes som en solid ekstern barriere.

e) Reversibilitet (manglende evne til at vende tilbage til systemet, som det var før ændringen)

Ændringen kan siges at være reversibel, hvis den tidligere SW version kan genindsættes uden at forandre sikkerhedsniveauet og uden at øvrige ændringer samtidig skal ske.

f) Akkumulation (vurdering af ændringens signifikans under hensyntagen til alle nylige sikkerhedsrelaterede ændringer, som ikke blev anset for signifikante, af det system, der er taget op til vurdering)

Tidligere ikke signifikante ændringer i CSM systemet skal medregnes, uanset om der er tale om SW eller HW ændringer.

Godkendelse og tilsyn

14. Trafik- og Byggestyrelsens behandling

Trafik- og Byggestyrelsens vejledninger om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen og godkendelse af køretøjer finder også anvendelse for delsystemer og køretøjer, hvori der indgår SW. Nedenstående vejledning skal ses som et supplement hertil.

Ændringsforelæggelse

Såfremt SW ændringen er signifikant eller at betragte som fornyelse eller opgradering, skal ændringen forelægges Trafik- og Byggestyrelsen, jf. BEK 653, § 12 eller BEK 661, § 9. Dette sker ved at indsende en projektbeskrivelse, som beskrevet i bekendtgørelserne. Nedenstående tabel viser kravene til projektbeskrivelsen, for køretøjer og for delsystemer i infrastrukturen:

ÆNDRINGSFORELÆGGELSE JF. BEK 653 OG 661.	
BEK 661, om ibrugtagningstilladelse for delsystemer i jernbaneinfrastrukturen. /2/.	BEK 653, om godkendelse af køretøjer på jernbaneområdet. /1/.
§ 9. I tilfælde af en ændring af et eksisterende delsystem, der vurderes at være signifikant eller som betragtes som fornyelse eller opgradering jf. § 7, stk. 2 eller 3, indsendes en projektbeskrivelse til Trafikstyrelsen, inden ændringen iværksættes. Trafikstyrelsen træffer afgørelse om, hvorvidt ændringen kræver en ny ibrugtagningstilladelse i henhold til § 6. *Stk. 2.* Projektbeskrivelsen skal indeholde følgende: 1) Dokumentation for virksomhedens vurdering om ændringens signifikans, jf. § 7. 2) **En foreløbig systemdefinition** af ændringen af delsystemet, herunder oplysninger om: a) virksomheden ønsker at anvende dokumentation fra en tilsvarende ændring, som tidligere har opnået en godkendelse i Danmark, et EU- eller EØS-land efter identiske krav under tilsvarende driftsbetingelser, og b) hvorvidt ændringen efter virksomhedens vurdering er omfattet af TSI-krav.	**§ 12.** I tilfælde af en ændring af et køretøj, eller en ændring af en godkendt køretøjstype, jf. § 11, indsendes en projektbeskrivelse til Trafikstyrelsen inden ændringen iværksættes. Trafikstyrelsen træffer herefter afgørelse om, hvorvidt der kræves en ny ibrugtagningstilladelse, eller en ny typegodkendelse og i hvilket omfang § 8 skal anvendes. *Stk. 2.* Projektbeskrivelsen skal indeholde følgende: 1) Dokumentation for forslagsstillers vurdering af ændringens signifikans, jf. § 11, stk. 1. 2) **Foreløbig systemdefinition** af ændringen, herunder oplysninger om: a) hvorvidt virksomheden ønsker at anvende dokumentation fra en tilsvarende ændring, som tidligere har opnået en godkendelse i Danmark, et EU- eller EØS-land efter identiske krav under tilsvarende driftsbetingelser, b) hvilke TSI-krav, der berøres af ændringen og hvilke TSI-krav der forventes anvendt, hvis ændringen efter virksomhedens vurdering er omfattet af en TSI, c) hvilke notificerede nationale tekniske regler, der berøres af ændringen og hvilke notificerede nationale tekniske regler, der forventes anvendt, og d) hvilke verifikationsprocedurer, virksomheden ønsker at benytte. 3) Foreløbig risikoanalyse.

Når det drejer sig om softwareændringer, bør den foreløbige systemdefinition udarbejdes i overensstemmelse med nærværende vejlednings kapitel 10. Derudover anbefales det at projektbeskrivelsen også vedlægges:

1) Vurderingen af ændringens kritikalitet.
2) ASRs vurdering af 1).
3) Oplysning om hvorvidt evt. eksisterende attester skal opdateres.

Assesmentrapporternes indhold

AsBos rapport

I det tilfælde hvor AsBo også har kompetencer og ressourcer til at agere ASR, kan sikkerhedsvurderingsrapporten enten have et selvstændigt afsnit vedr. opfyldelsen af EN50128 eller en reference til en selvstændig software assessment rapport, som vedlægges.

I det tilfælde hvor AsBo ikke selv forestår EN50128 assesseringen gælder følgende vejledning: AsBo bør kontrollere, at ASRs rapport kan anvendes som dokumentation for, at CSM sikkerhedskrav og SIL, kan anses for at være opfyldte. AsBo bør desuden sikre sig, at ASR har anvendt kompetente fagassessorer. Resultatet af denne kontrol bør fremgår af sikkerhedsvurderingsrapporten. ASRs assessmentrapport vedlægges sikkerhedsvurderingsrapporten.

ASRs rapport

ASRs SW assessementrapport bør udarbejdes i overensstemmelse med EN50128 kapitel 6.4. Rapporten bør bl.a. indeholde:

- Identifikation af SW og version(er)
- Assessment af hvordan EN50128 er anvendt
- Assessment af anvendelsesbetingelser for SW fx:
    - Krav til installation og test
    - Krav til konfigurations- og ændringsstyring
    - Øvrige sikkerhedsmæssige anvendelsesbetingelser (SRAC)
- Assessors supplerende anvendelsesbetingelser
- Hvad der godt må ændres i uden fornyet assessment

Ikke signifikante SW ændringer

Som vist i procesmodellen kan der forekomme tilfælde, hvor en SW ændring er ”major” eller ”minor” men ikke signifikant. I disse tilfælde bør jernbanevirksomheden/infrastrukturforvalteren, ud over signifikansvurderingen, opbevare fabrikantens kritikalitetsvurdering, og den tilhørende ASR vurdering. TBST kan ved tilsyn efterspørge disse dokumenter.

Såfremt der er tale om en ”major” SW ændring, bør der også foreligge en positiv ASR assessment rapport. TBST kan ved tilsyn efterspørge rapporten.

Håndtering af `ukurant´ SW

15. Systemer med SW 'proven in use'

Eksisterende ældre SW kan være udviklet uden brug af EN50128 og/eller uden brug af et fastlagt SSIL niveau for SW sikkerhedsfunktionerne. Sikkerheden i systemer med anvendelse af SW uden brug af EN50128 er ofte baseret på procedurer, der ikke er dokumenterede suppleret med vidtgående test af den pågældende SW i stedet for systematiske processer. Disse forhold kan gøre det mere udfordrende at ændre softwaren, når principperne i nærværende vejledning samtidigt bør følges:

Systemdefinitionen

Vejledningens anbefalinger i kapitel 10 om hvorledes systemdefinitionen bør udformes, er ikke baseret på EN50128, og kan også anvendes for ukurant SW. Men det kan være en udfordring at fremskaffe dokumentation for CSM systemet, herunder sikkerhedskravene. Det er imidlertid nødvendigt for at kunne ændre det på en forsvarlig måde.

Kritikalitetsvurderingen

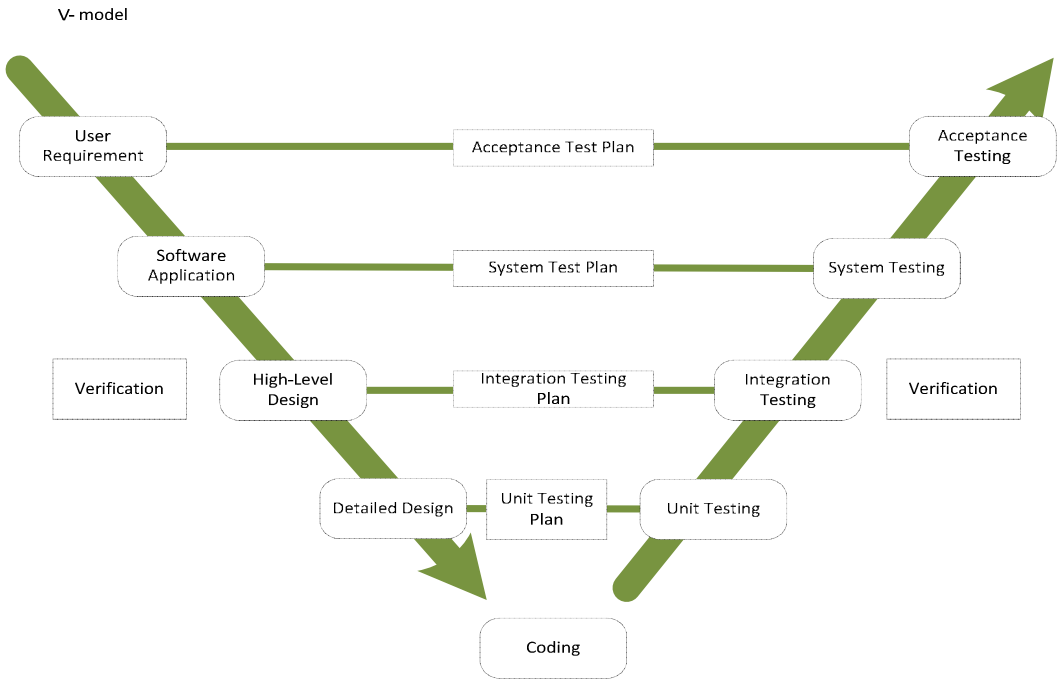
Fremgangsmåden til bestemmelse af softwareændringens kritikalitetet, beskrevet i bilag 1, er ikke afhængig af, at EN50128 anvendes. Kritikalitetsvurderingen vil derfor også kunne laves for ældre SW. Men det kan være en udfordring at beskrive SW arkitekturen mv., hvis der ikke allerede foreligger dokumentation herfor. Det er imidlertid nødvendigt for at kunne ændre softwaren på en forsvarlig måde.

Signifikansvurderingen

Ændringer i ukurant sikkerhedsrelateret SW skal altid signifikansvurderes. Vejledningens afsnit om signifikansvurdering og bilag 1 er ikke baseret på at EN50128 anvendes, og kan derfor også anvendelse til vurdering af ukurant SW.

Udviklingsprocessen

SW udvikling bør altid følge en egnet procedure, og den såkaldte V-model er et eksempel herpå. Se nedenstående Figur 11 V-model for udvikling.



Figur 11 V-model for udvikling

Såfremt den eksisterende SW er udviklet efter en dedikeret og dokumenteret procedure, bør den normalt også følges, når der laves ændringer.

Ellers kan der tages udgangspunkt i EN50128, men det kan være en udfordring at specificere SW kravene, hvis den eksisterende SW er en "black box". Dette kan i nogen grad kompenseres ved at lave en omfangsrig testplan.

Assessering

Uagtet om EN50128 følges eller ej, bør der altid involveres en SW assessor, når der ændres i SW som indgår i sikkerhedskritiske systemer. Assessors opgaver er i princippet de samme, som når EN50128 anvendes. I de tilfælde hvor EN50128 ikke følges, bør assessor dog også forholde sig til om udviklingsmodellen er egnet.

Bilag 1: Bestemmelse af kritikalitet

Dette bilag beskriver en procedure, som kan anvendes til fastlægning af, om der er tale om en minor eller major SW ændring. Proceduren er ikke afhængig af, om man anvender EN50128, eller en anden egnet proces, men anvender man EN50128 kan proceduren netop anvendes til at få fastlagt minor eller major, da EN50128, som tidligere omtalt, ikke fastlægger principper for bestemmelsen heraf.

Kritikalitet er knyttet til det, der i standarderne hedder Safety Integrity Level (SSIL) som nærmest kan beskrives som en målestok for, hvor sikker man skal være på, at en bestemt funktion faktisk virker, når der er brug for, at den virker. Implicit betyder dette, at et højt Safety Integrity Level normalt også betyder, at SW er meget kritisk og dermed vil en ændring af SW hurtigt være en major ændring. I proceduren er der defineret visse undtagelser for denne grundregel.

I proceduren indgår bestemmelsen af *sikkerhedsintegritet, forudbestemt variant* og *simplicitet*, hvilket er nærmere beskrevet nedenfor.

SW design

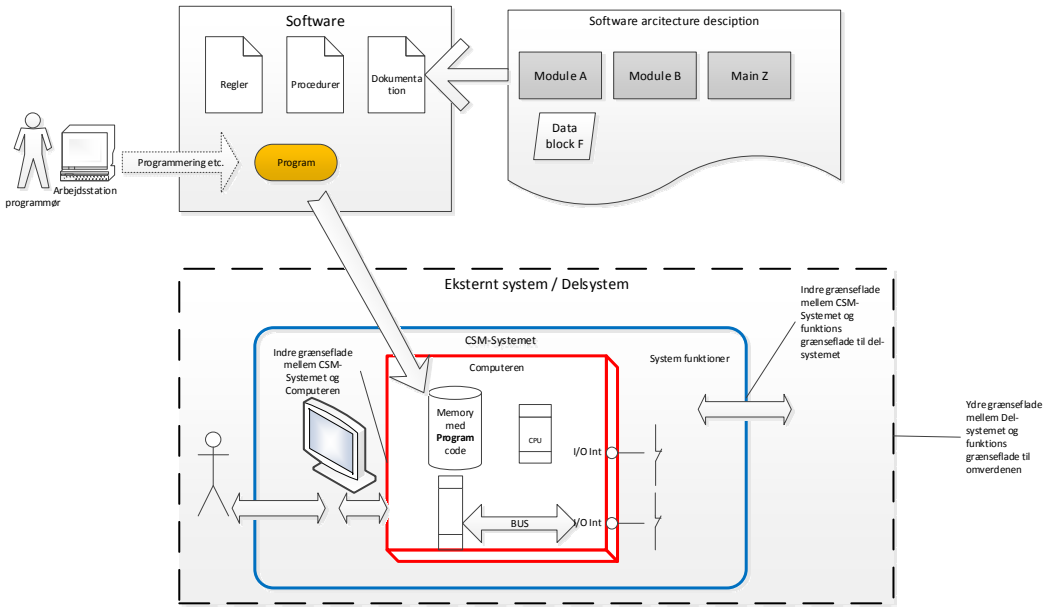
Inden kritikaliteten kan bestemmes, skal systemdefinitionen (Se kapitel 10), suppleres med en nærmere beskrivelse af softwaren for visse af overskrifterne, som følger:

b) systemfunktioner og –elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationelle elementer)

Nedenstående liste tjener til at præcisere det, der især er relevant, når kritikalitet skal vurderes:

- Blokdiagram der viser samspillet mellem evt. flere computere
- Computerens SW arkitektur (System architecture description jf. EN50128)
- Berørte SW moduler (Components jf. EN50128)
- Berørte SW sikkerhedsfunktioner
- Evt. tilstandsdiagrammer
- Evt. menneskelig interaktion og betjening
- Evt. computerens HW arkitektur
- Udviklingsmiljøet og SW-værktøjer.

Se også nedenstående figur.



Figur 12 Blokdiagram i systemdefinition

c) systemafgrænsning, herunder vekselvirkninger med andre systemer

Det er vigtigt at beskrive hvilke dele der med logiske argumenter kan siges at være uberørte. Fx nabo computere uden bus forbindelse til aktuel computer, anvendte værktøjer, HW, osv.

Følgende beskrives:

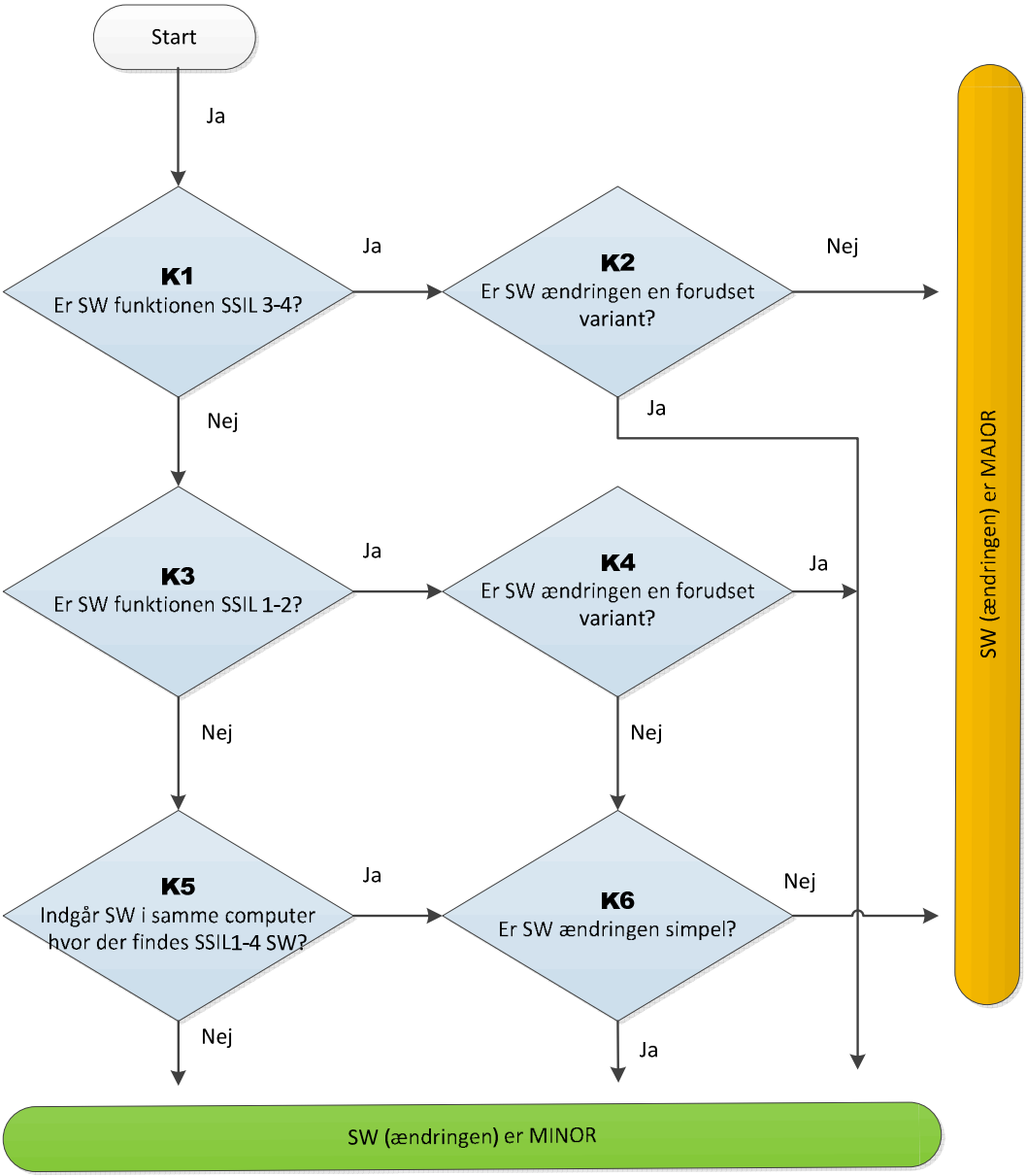
- Grænsefladen fra den installerede SW til SW-udviklingsværtøjer
- Grænsefladen til upload af nyt / ændret program
- Skitser der viser hvordan SW i samme computer evt. ikke kan berøres ved ændringen.

g) antagelser med henblik på at afgrænse kritikalitetsvurderingen

Her kan fx anføres yderligere antagelser om det valgte programmeringssprog, compiler, assembler, computeren osv.

Bestemmelse af kritikalitet

Kritikaliteten kan bestemmes i overensstemmelse med Figur 13, nedenfor.



Figur 13 Bestemmelse af kritikalitet

Bestemmelse af sikkerhedsintegriteten (K1 og K3)

Er SSIL-værdien ikke kendt, kan fastlægningen ske ved at anvende EN50129 Annex A eller IEC 61508. Som støtte til dette kan nedenstående tabel i udgangspunkt anvendes.

Computerens sikkerhedsfunktioner vedrører	**Typisk fastlagt SSIL**	**Bemærkninger**
Sikringsanlæg (Objektstyring, centralsikring osv.)	4	
Togkontrol: ETCS, CBTC, ATC, HKT onboard	4	
Togdetektering akseltællere, mv.	4	
Baliser	4	Bestemmelsen afhænger af systemkonceptet. SSIL kan godt være fx 1-2, hvis flere baliser indgår.
Togcomputer med direkte styring af togets sikkerhedsfunktioner, hvor fejl i SW fx kan medføre kollision	3	
Togcomputer der overvåger eller indirekte styrer togets sikkerhedsfunktioner.	2	
Objekt og persondetektorer (spor og perron etc), kamera mønstergenkendelse osv.	1	
Varmtløbs detektering	1	
Brandalarmer, motorstyring og kommunikation i tog	1	
Bremsecomputere, WSP systemer	1	SSIL 1 forudsætter at nødbremsesystemet er helt uafhængigt af disse systemer. Er det ikke tilfældet vil SSIL typisk være 3-4.
TMS, TCM, CTC, TCC (fjernstyring) Kørestøms- og kobler styring SCADA systemer (overvågning og styring)	1-4	Systemerne har ofte meget få sikkerhedsfunktioner, og tit kan det vises at SSIL 0 er tilstrækkeligt. SSIL er her sat fra 1 til 4, da der ofte løses visse sikkerhedsfunktioner. For S-banen (CBTC systemet) er der sikkerhedsfunktioner i SSIL 4 niveau.
Omstillingsanlæg for rangerbanegårde	1	
Informationssystemer, klimaanlæg, meldedisplays osv.	0-2	EN50128 er, jf. afsnit 1.3 i standarden, ikke relevant for SW, der er identificeret som uden betydning for sikkerheden, dvs. SW som i tilfælde af SW fejl, ikke kan påvirke nogen sikkerhedsfunktioner. Informationssystemer, og klimaanlæg der måtte have betydning for sikkerheden, er omfattet af standarden. ETCS DMI er fx SIL 2.

Tabel 2 Bestemmelse af SSIL

Forudbestemt variant (K2 og K4)

En forudbestemt variant er en ændring, der på forhånd er omfattet af det certificerede og godkendte system. Den forudbestemte variant kan indgå som en del af SW maintenance planen, jf. EN50128.

SW som ændres, kan fx vedrøre datafelter, datablokke, kodefelter mv. sådan, at en på forhånd kendt egenskab/ydelse opnås ved, at en i programmet kendt programkode aktiveres eller afvikles på en anden måde. Følgende vejledning gælder for bestemmelsen:

1. Ændringen skal være 'lovlig', hvilket vil sige, at handlingen er omfattet af en eksisterende assessment / godkendelse / certificering (ved et/en NoBo/DeBo/køretøjssagkyndig).
2. Ændringen følger nogle på forhånd fastlagte regler og implementeringsprocedurer.

Er det tilfældet, kan ændringen siges at være en forudbestemt variant.

Eksempel 1
En vejlængdemåler (Odometer) kan indstilles til forskellige hjuldiametre, hvor ændringen består i at udskifte et kodefelt fx en chip med de nye data for hjuldiameteren. Det bagvedliggende program er godkendt til at håndtere nye input fra kodefeltet.

Eksempel 2
Et sikringsanlæg er designet så SW kan styre henholdsvis et, to eller tre sporskiftedrev. Når der ændres i antallet af drev, er det en værdi i en parameter i SW, der ændres.

Eksempel 3
Et overkørselsanlæg er designet, så SW kan styre henholdsvis en eller to bomme, og/eller et eller to spor. Når der ændres i antallet af spor og bomme, er det nye parametre i SW, der ændres.

Eksempel 4
Et dørstyringssystem er designet, så SW kan styre både døre med skydetrin og døre uden. I computeren bestemmes dette af en manuel switch.

Bestemmelse af simplicitet (K6)

Visse ændringer kan tillægges værdien 'simpel'. Imidlertid kan en tilsyneladende simpel SW ændring let have nogle uhensigtsmæssige og uoverskuelige følgevirkninger, hvis ikke ændringen sker i et meget kontrolleret SW miljø. Fx kan en lille fejlrettelse i et program påvirke andre dele af samme program både som følge af at programmet selv påvirker det andet program eller som følge af, at programmet anvender samme HW fx datalager mv.

EN50128 har i Appendix D.32 'Impact analysis' beskrevet nogle krav til overvejelser, der skal foretages, når SW ændres. Overvejelserne munder bl.a. ud i en analyse og beslutning om, hvor meget af SW, der ændres, og hvor meget der på ny skal valideres og testes. Disse dokumenterede analyser kan ligge til grund for simplicitetsbestemmelsen.

Alternativt vil følgende altid kunne anvendes for bestemmelsen:

1. Ændringen skal vedrøre en fejlrettelse eller modifikation[15] i kun et programmodul.
2. Ændringen skal være 'indkapslet' i en SW arkitektur, hvor det kan bevises, at ændringen ikke kan have sideeffekter eller afsmitte på anden programkode.
3. Det skal kunne sandsynliggøres (jævnfør EN50128 kapitel 7.5) at ændringen er tilstrækkelig testbar.

Ad 1: En fejlrettelse betyder, at modulet ikke opfører sig som specificeret og ændringen heri er at få modulet til at opføre sig korrekt. Er der tale om en modifikation, vil der også være en ny specifikation af, hvordan modulet skal fungere. Modulet har entydige grænseflader, og der er hverken flere eller færre grænseflader efter modifikationen.

Ad 2: Det kan imidlertid være vanskeligt at foretage egentlige afgrænsninger af SW, og hvis der er tale om et 'single processor system' er man som regel nødt til at betragte alt SW til compute-

[15] Generelt kan flere samtidige rettelser ikke anvendes inden for bestemmelsen idet disse hurtigt bliver en kompleks rettelse.

ren. Såfremt der findes fastlagte systematikker for hvordan 'indkapslingen' fungerer, og ASR er enig i dette, opfyldes punktet.

Ad 3: Ved at opstille kriteriet fra 1. og 2. kan det kombineret med EN50128 kapitel 7.5 om 'test coverage' vises, at modulet er tilstrækkelig testbart, hvilket vil sige alle inputkombinationer, og alle output er kendte og testbare.

Er det tilfældet, kan ændringen siges at være simpel.

Software i samme computer (K5)

Hvis computeren indeholder flere typer programmer, hvor noget løser sikkerhedskritiske funktioner (SSIL 1-4) og andet ikke gør, er det ofte vanskeligt at adskille og påstå, at man kun ændrer i det, der ikke er kritisk (SSIL 0). Argumentationer bør derfor begrænses til systemer, som kun indeholder SSIL 0.

Bilag 2: Eksempel på ændring af `ukurant´ SW

Indhold

Indledning

Dette bilag indeholder et eksempel på en ændring af en eksisterende `ukurant´ software i et passager-informationssystem (PIS) i et tog.

Informationssystemet sikrer kommunikationen mellem lokomotivfører, togfører og passagererne.

Systemdefinitionen

Forslagsstiller (her en jernbanevirksomhed) udarbejder systemdefinitionen jf. vejledningens kapitel 10:

a. En systemmålsætning, f.eks. det tilsigtede formål

I denne case antages, at der i gennem et års driftserfaringer er opstået et behov for at ændre PIS-softwaren. Der er et par ændringer: a) en særlig driftssituation med koblet-tog, hvor kommunikation mellem lokomotivfører og togfører fungerer ulogisk og b) tilslutning af en ny type håndsæt.

b. Systemfunktioner og –elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationeller elementer)

Funktioner

PIS-systemet indeholder et antal funktioner:

- Lokomotivfører-beskeder til passagerer (selektiv og global PA*)
- Samtaleanlæg mellem lokomotiv- og togfører (selektiv og global IC*)
- DVA (automatisk højtaler information: 'Næste station er..')
- Display styring (intern og ekstern)
- Pladsreservation
- Nødtale-enheder (ikke nødbremsehåndtag)

* med selektiv/global menes, om beskeden gives til en bestemt vogn / alle vogne i toget. PA ='Public Announcement' og IC = InterCommunication mellem f.eks. togfører og lokoførere.

Under normal drift er funktionerne ikke sikkerhedsrelaterede, f.eks. en global PA med 'Besked om forsinkelse'.

I nødsituationer bliver kommunikationen dog sikkerhedsrelateret, f.eks. skal lokomotivføreren kunne annoncere en evakuering via global PA i tilfælde af brand i en tunnel.

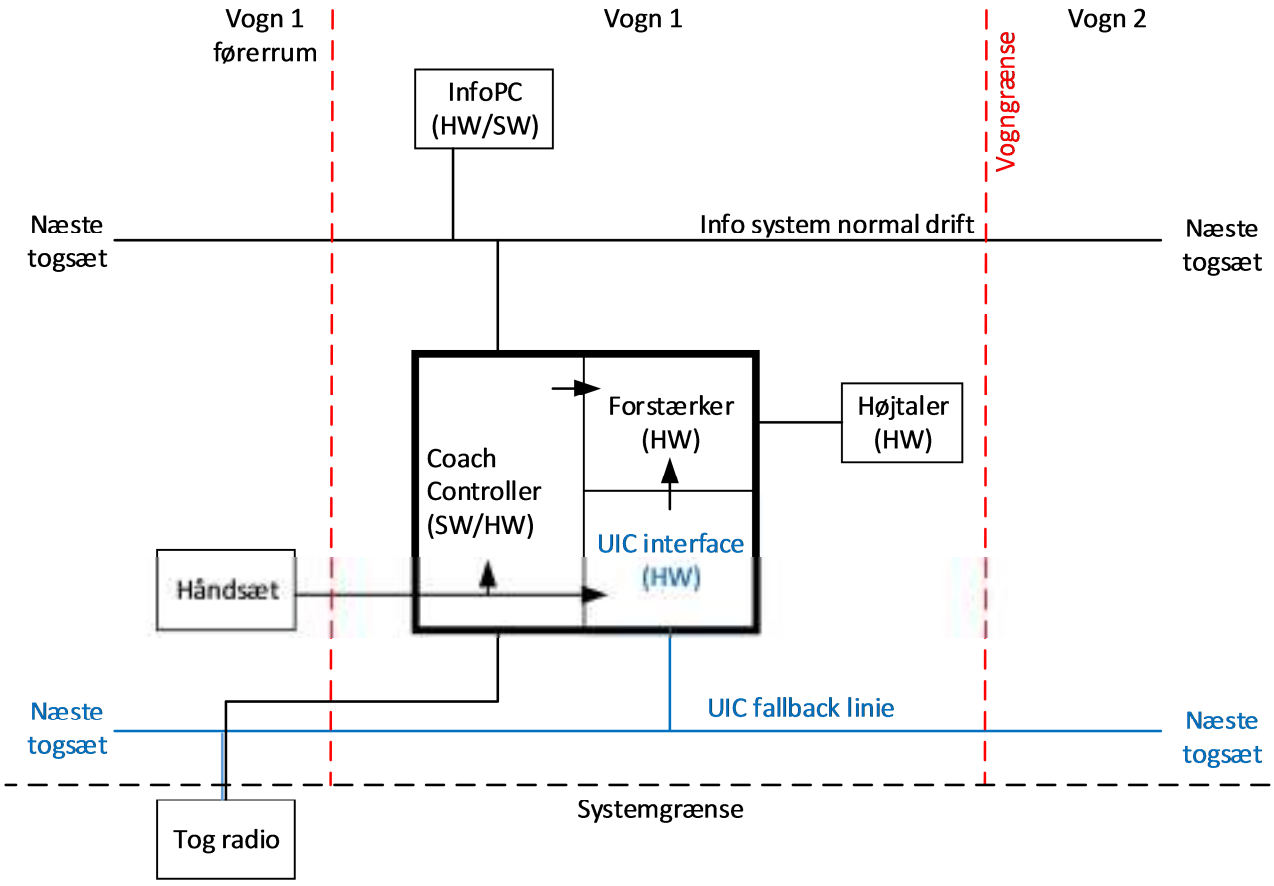
Elementer

På figur 14 nedenfor er vist et basis PIS-system. De sorte bokse og streger på figuren er PIS-systemet, som er SW-baseret, dvs. alle funktionerne udføres af den samlede SW i de forbundne controllere.

PIS-systemet kan udvides med et rent hardwarebaseret 'UIC-system', hvor UIC-systemet er de blå bokse og streger. Dette udvidede system kaldes PIS+UIC og består således af det samlede sorte og blå system.

I PIS+UIC-systemet er det muligt at udføre funktionerne global PA og global IC både via det sorte softwarebaserede PIS-system og via den blå UIC hardwarelinje.

Det afhænger af togtypen, om der køres med PIS eller PIS+UIC.



Figur 14 Systemdefinition for PIS.

PIS er det sorte system. Det blå UIC system er en udvidelse til PIS-systemet. (Forkortelserne på figuren står for SW/HW = soft-/hardware, UIC = en standard HW kommunikationslinje.)

c. Systemafgrænsning, herunder vekselvirkning med andre systemer

PIS-systemet er et autonomt teknisk system med en teknisk grænseflade til tog-radioen.

Der er flere direkte menneskelige grænseflader mod lokomotiv- og togfører og passagerer.

d. Fysiske (dvs. vekselvirkende systemer) og funktionelle (dvs. funktionelt input og output) grænseflader

Se figur 14.

e. Systemmiljøet

PIS-systemet hører ind under kategorien for EN50155, 'Electronic equipment used on rolling stock'. Denne standard sætter rystetest, brandkrav, EMC mv.

Det bemærkes, at EN50155 også indeholder simple ISO-kvalitetskrav til softwaren.

f. Eksisterende sikkerhedsforanstaltninger, og efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen.

PIS-systemet er ældre, og den oprindelige SW blev udviklet, før EN50128 blev frigivet. Systemet er "proven in use".

Som beskrevet ovenfor samler den sikkerhedsmæssige interesse sig om global-PA og -IC funktionerne. I det følgende benævnt 'G-PA/IC'.

G-PA/IC funktionernes sikkerhedsintegritet, på funktionsniveau, bestemmes til SIL1, jf. IEC 61508. Den vejledende tabel 2 i bilag 1[16] 'Bestemmelse af SSIL' anvendes til kontrol heraf.

Bemærk, at SIL-bestemmelsen gælder på funktionsniveau og er uafhængig af om den implementeres med PIS eller PIS+UIC systemet.

Dette kan, nedbrydes til følgende HW/SW krav:

System	G-PA/IC funktionernes sikkerhedsintegritet, på systemniveau	HW-krav	SW-krav
PIS	SIL1	SIL1	SSIL1

g. Antagelser med hensyn til at afgrænse risikovurderingen

I denne case leveres PIS-softwaren af en kendt leverandør. Rettelser i SW'en udføres af en programmør, som kender det ældre udviklingsmiljø. Testmiljøet er velprøvet.

Risikovurderingen nedenfor er lavet for PIS-systemet alene, og omfatter således ikke PIS+UIC systemet.

Procesmodellen (I) – Forudsætninger for processen

Vejledningens procesmodel forudsætter følgende:

1. At ændringen vedrører software.
2. At SW har indflydelse på sikkerhed eller interoperabilitet.
3. Ændringen udføres under SLS/ QMS af kompetente personer.

Som det fremgår af ovenstående gennemgang af PIS-systemet, er startbetingelse nr. 1. – 3[17]. opfyldt, og procesmodellen (II) kan derfor anvendes.

Procesmodellen (II) – Flowdiagram

Nedenfor gennemgås kapitel 'Procesmodellen (II) – Flowdiagram' fra vejledningen.

[16] Bemærk at tabellen er en støtte tabel. SIL kan fastlægges ved at anvende EN50129 Annex A eller IEC 61508.

[17] I eksemplet er der ikke udførligt redegjort for SLS / QMS og kompetencer. Disse forhold forudsættes at være under kontrol.

Trin	Emne	Beskrivelse /analyse	Resultat
A	Startbetingelse	Projektlederen for 'Ændring af PIS-system' er placeret hos operatørens underleverandør af vedligehold.	
B	Udarbejd system-definition	Denne er (overordnet) udarbejdet ovenfor.	
C	Fastlæg signifikans	Ændringens kritikalitet, vurderes af SW leverandøren, og hans SW assessor ud fra principperne i vejledningens bilag 1. Det forudsættes her, at der er tale om en minor ændring. Herefter kan signifikansen bestemmes: Fra vejledningens kapitel 'Bestemmelse af signifikans'. Konsekvens: Alvorlig; hvis G-PA/IC svigter ved scenario 'Brand i tunnel'. Nyskabelse: Lav; da kendt udviklingsmiljø og ingen nyskabende funktioner. Kompleksitet: Lav; da ændringen er minor. Overvågning: Høj; da operatørens eksisterende procedurer foreskriver daglig test af G-PA/IC. Reversibilitet: Høj; da relativt nemt at skifte til tidligere SW-version. Akkumulation: Nej. I eksemplet er der ikke udført tidligere ændringer. Vurdering. Ikke signifikant; Alvorlig konsekvens taler for signifikant, men især pga. høj overvågning og da de andre parameter taler for ikke-signifikant, vurderes ændringen ikke-signifikant.	
E	Er systemet omfattet af TSI eller NNTR krav?	TSI Loc&Pas stiller både krav til sikkerhedsrelateret SW (se kapitel 11 i vejledningen) og til kommunikationssystemer.	=>H
H	Kritikalitet (Minor / Major)	Ifølge flowchart i vejledningens bilag 1 er der tre krav til simplicitet (K6): 1) Fejlrettelse 2) Indkapslet 3) Høj testbarhed i softwaren af G-PA/IC Selve PIS-systemet er autonomt og dermed indkapslet. Ændringen vedrører en fejlrettelse og en intern grænsefladekomponent. Sikkerhedsfunktionen G-PA/IC og den nye komponent har høj testbarhed, så alt i alt vurderes ændringen som simpel. Det er nu muligt at afgøre, at ændringen er minor, idet K1=nej; K3=ja; K4=nej og K6=ja. Vurderingen forelægges ASR, i overensstemmelse med EN50128.	=>G
G	Nyt delsystem eller fornyelse eller opgradering?	Der er ikke tale om et nyt delsystem. Ordregiver (her jernbanevirksomheden) vurderer at der ikke er tale om fornyelse eller opgradering, jf. kriterier nævnt i pkt. G i procesmodellen.	=>F
F	Skal systemet certificeres?	Nej, da systemet ikke i forvejen er certificeret. Hvis systemet havde været certificeret af NoBo, skulle NoBo have vurderet certifikatets fortsatte gyldighed jf. vejledningens kapitel 12.	=>K
K	Er ændringen signifikant eller er det et ny delsystem?	I eksemplet er der tale om en ikke signifikant ændring af det eksisterende delsystem "rullende materiel".	=>M
M	Kritikalitet?	Se H.	=>P

Trin	Emne	Beskrivelse /analyse	Resultat
P	Anvend EN50128 kapitel 9.2	EN50128, kapitel 9.2, henviser til ISO/IEC 90003 standarden, som er en kvalitetsstyringsstandard for SW. Se også kapitel "Håndtering af ukurant SW".	
S	Systemet ibrugtages i overensstemmelse med jernbanevirksomhedens og/eller infrastrukturforvalterens SLS.	Jernbanevirksomheden opbevarer bl.a.: - Signifikansvurderingen og systemdefinitionen. - Leverandørens kritikalitetsvurdering. - SW assessors vurdering af kritikalitetsvurderingen.	

Tabel 3 Gennemgang af flowdiagram i vejledningens kapitel 'Procesmodellen (II) – Flowdiagram'

Bilag 3: Eksempel på ændring i CBTC on-board

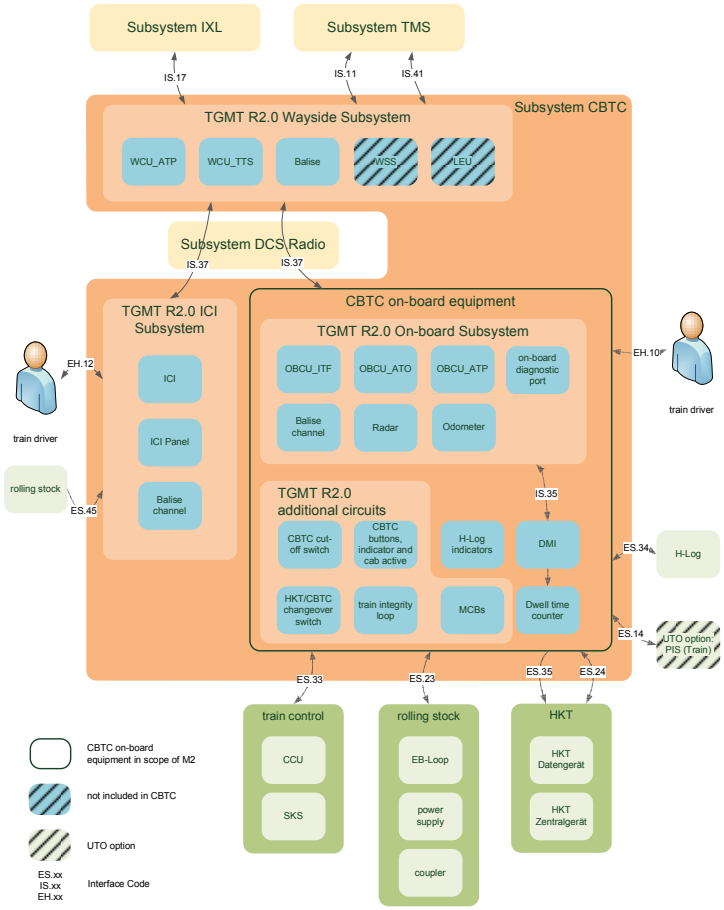
Indhold

Indledning

Eksemplet tager udgangspunkt i en kendt ændring af ombordudrustningen på Københavns S-bane. Ændringen er beskrevet i en systemdefinition 'SW Change to Onboard S-tog M1.99 Variant', Siemens doc: A6Z00037537227. Her kaldt SYSDEF. Udrustningen kaldes 'CBTC on-board equipment' og ses helt overordnet i den sorte ramme i nedenstående figur.

Af figuren fremgår det også, at udrustningen består af flere computere og en ændring i delsystemet mobilt togkontrol kan berøre SW i en eller flere computere. Opbygningen er meget kompleks, og en ændring i en computer kan både have indflydelse på andre dele af 'CBTC on-board equipment' og S-banens faste CBTC system.

Den i eksemplet anvendte ændring kan karakteriseres som mindre funktions- og fejlrettelse. Ændringen foretages i forskellige SW moduler, som kører på forskellige computere i det mobile CBTC system.



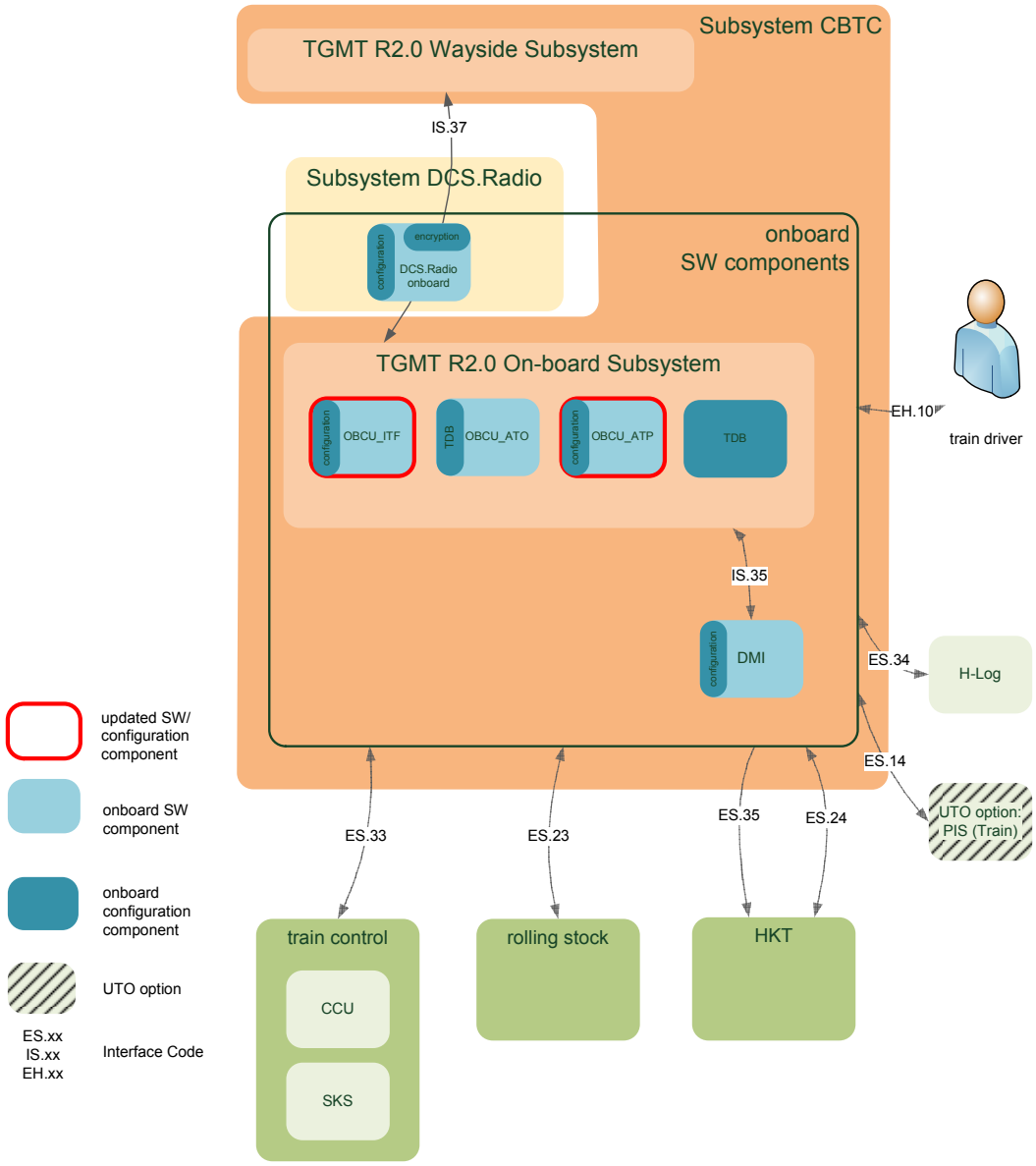
Eksemplets Systemdefinition

a. en systemmålsætning, f.eks. det tilsigtede formål

S-tog onboard database skal bringes i overensstemmelse med infrastrukturen samt rettelse af fejl.

b. systemfunktioner og –elementer, når dette er relevant (herunder eksempelvis menneskelige, tekniske og operationelle elementer)

I blokdiagrammet nedenfor ses det overordnede delsystem hvor computerne / SW i computerne befinder sig.



De røde markeringer viser der, hvor ændringerne sker. Af SYSDEF fremgår hvilke specifikke korrektioner i SW, der laves. Der er ingen egentlige funktionsændringer og sikkerhedsfunktionerne ønskes bibeholdt.

Computerens SW arkitektur og de berørte SW moduler fremgår af Siemens dokumentationen via en henvisning.

Samtlige ændringer i SW er oplistet i form af en "fix request". Der er ingen ny menneskelig interaktion og betjening.

c. systemafgrænsning, herunder vekselvirkninger med andre systemer

Systemafgrænsningen er overordnet vist på figuren.

I eksemplet er CSM- og delsystemet det samme eftersom alt er fuldt integreret og der foretages ændringer i alle dele.

d. fysiske (dvs. vekselvirkende systemer) og funktionelle (dvs. funktionelt input og output) grænseflader

Der er som udgangspunkt ingen ændringer. SYSDEF henviser til gældende systemtegning for S-togs udrustningen

e. systemmiljøet (f.eks. energi- og varmestrømme, stød, vibrationer, elektromagnetisk interferens, operationel anvendelse)

Uforandret

f. eksisterende sikkerhedsforanstaltninger og, efter en iterativ proces, definition af de sikkerhedskrav, der er identificeret i forbindelse med risikovurderingsprocessen

De fleste eksisterende sikkerhedsfunktioner er fastlagt til SIL 4 og de forudsættes uforandrede efter ændringen.

SYSDEF henviser til kravspecifikationen for hele 'onboard'.

g. antagelser med henblik på at afgrænse risikovurderingen

Da der ikke er identificeret nye sikkerhedsfunktioner antages det, at alle krav er uforandrede.

Procesmodellen (I) – Forudsætninger for processen

Vejledningens procesmodel forudsætter følgende:

1. At ændringen vedrører software.
2. At SW har indflydelse på sikkerhed eller interoperabilitet.
3. Ændringen udføres under SLS/ QMS af kompetente personer.

Ad 1.: Jf. SYSDEF : "system definition for SW change" er der tale om en SW ændring.

Ad 2.: Da der ændres i SSIL 4 klassificeret SW, kan sikkerheden påvirkes.

Ad 3.: Organisation er uforandret i forhold til den øvrige introduktion af CBTC på S-banen.

Konklusion: Startbetingelse nr. 1. – 3. er opfyldt, og procesmodellen (II) kan derfor anvendes.

Procesmodellen (II) – Flowdiagram

Nedenfor gennemgås kapitel 'Procesmodellen (II) – Flowdiagram' fra vejledningen.

Trin	Emne	Beskrivelse / analyse	Resultat
A	Startbetingelser	Disse er opfyldt, som beskrevet under Procesmodellen (I).	
B	Systemdefinition	Er udarbejdet. Se tidligere afsnit.	
C	Er systemet omfattet af TSI/NNTR?	S-banen, og køretøjer som alene anvendes her er undtaget fra IOD.	=>D
D	Indgår SW i et køretøj?	I dette eksempel; ja.	=>F
F	Skal systemet certificeres?	Ombordudrustningen, som ændres, er certificeret v/en køretøjssagkyndig. Ændringen forelægges den køretøjssagkyndige som i dette eksempel afgør at der skal laves nye attester, da de eksisterende attester mister deres gyldighed pga. ændringen.	=>I
I	Systemet certificeres	Den sagkyndige opdaterer attesterne. Denne aktivitet behøver ikke tidsmæssigt at afsluttes for at forsætte til trin K.	
K	Er ændringen signifikant, eller er det et nyt delsystem?	a) Konsekvens af svigt Eksisterende SW er klassificeret som SIL 4. SW leverandøren klassificerer ændringen som "major" fordi der ændres i SIL 4 funktioner uden nogen forudbestemt variant. ASR er enig heri.	=> L

Trin	Emne	Beskrivelse / analyse	Resultat
		b) Nyskabelse Lang erfaring med ændringer i den pågældende SW SW er udviklet efter EN50128 og vurderet af ASR. Ændringen vil blive foretaget efter EN50128 og vurderet af ASR. Det introduceres ikke nyskabende funktioner. c) Ændringens kompleksitet Ændringer foretages flere steder og må siges at være kompleks. d) Overvågning Ikke muligt at forhindre ulykker. e) Reversibilitet Ikke mulig i drift, og fejl skal rettes. f) Akkumulation Ændringen er før IBT Konklusion Selv om b), nyskabelse, kan tale for at ændringen ikke behøver at være signifikant, taler a), c), d) og e) for at den skal vurderes som signifikant.	
L	Anvend CSM RA…	AsBo skal som minimum have: - Den nye systemdefinition - ASRs rapport.	
N	Kritikalitet	SW leverandøren klassificerer ændringen som ”major”. ASR er enig heri.	=>R
R	Anvend EN50128	Standarden anvendes af SW leverandøren. ASR vurderer resultatet heraf. Assesment rapporten sendes til AsBo som i dette tilfælde, udarbejder et tillæg til sikkerhedsvurderingsrapporten.	
K	Ændringsforelæg-gelse	Ændringen forelægges Trafik- og Byggestyrelsen, som, i dette tilfælde afgør at der skal udstedes en ny Ibrugtagningstilladelse efter bestemmelserne i BEK653, § 8.	

Tabel 4 Gennemgang af flowdiagram i vejledningens kapitel ’Procesmodellen (II) – Flowdiagram’

Vejledningen handler om hvordan jernbanens tekniske systemer med software skal håndteres med henblik på en myndighedsgodkendelse af nye systemer eller systemer der ændres.

Trafik- og Byggestyrelsen
Edvard Thomsens Vej 14
2300 København S
info@tbst.dk
www.tbst.dk