DK-STM

Systembeskrivelse

banedanmark

Verificeret	Adresse Banedanmark Amerika Plads 15 2100 København Ø	Projektering Siemens A/S Borupvang 3 2750 Ballerup	
Afløser			
Godkendt af Banedanmark			

	1. udgave Dato og initialer	Seneste udgave Dato og initialer	Tegningsnavn **DK-STM** Systembeskrivelse
Udarbejdet	23-01-2012 BBE	19-11-2014 BBE	
Kontrolleret	23-01-2012 STN	03-12-2014 STN	
Godkendt	23-01-2012 STN	04-12-2014 STN	

Sprog	Udgave	Tegningsnr	Side/af sider
DA	**2.00 19.11.2014**	KN 655.00 Q2959	1 (39)

Ændringslog

Udgave / dato	Omfattede sider	Beskrivelse	Referencer
01.00 / 23.01.2012	Alle	Første endelige udgivelse	
02.00 / 19.11.2014	Alle	Baseline 3.0 opdatering	

Indhold:

1 Indledning

Dette dokument udgør Systembeskrivelsen til komponenten DK-STM. DK-STM er en komponent der gør det muligt at et ETCS udrustet tog kan benytte ATC infrastrukturen. DK-STM indgår sammen med ETCS Onboard i et samlet ETCS system.

1.1 Formål

Dokumentet er skrevet til teknisk personale med ønske om at få et overblik over DK-STMs funktionalitet.

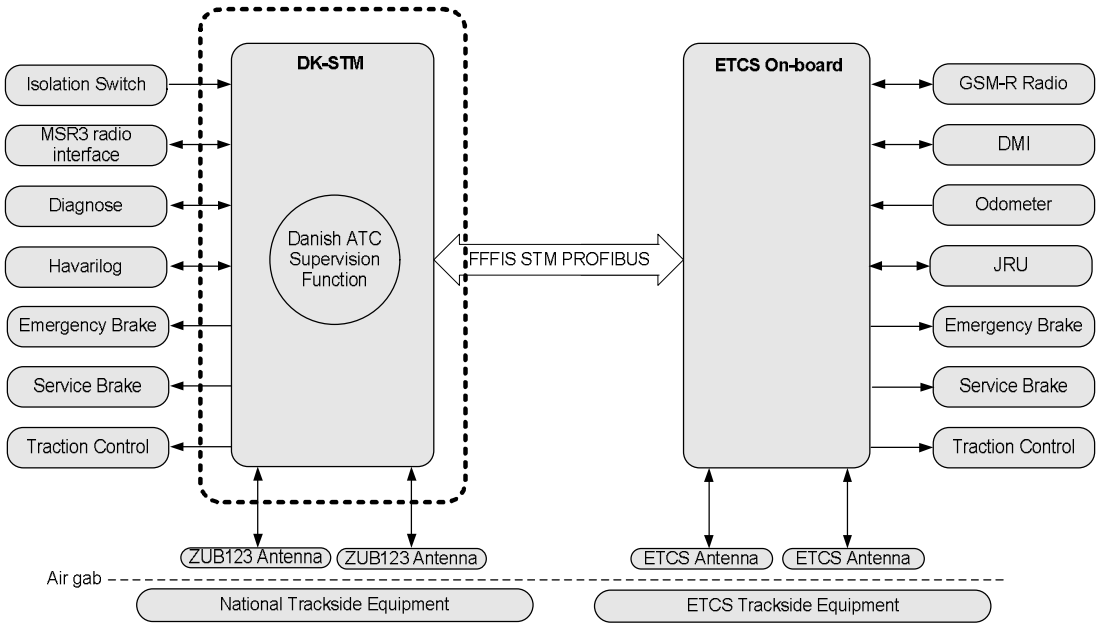
Formålet med dokumentet er at beskrive DK-STMs funktioner, således at læseren får en forståelse af, hvilke opgaver en DK-STM varetager i det samlede ETCS system.

Der bliver gennemgået hvilke komponenter, der er brugt for såvel hardware som software, samt det bliver klarlagt, hvorledes der ved forskellige processer og design opnås et SIL4 produkt.

Derudover gennemgås DK-STMs driftsmæssige tilstande og reaktioner på fejl.

1.2 Afgrænsninger

Dette dokument vil udelukkende omhandle funktionaliteten og egenskaberne for en DK-STM.



Figur 1: Afgrænsning af DK-STM Systembeskrivelse

På Figur 1 vises med den stiplede linie rammerne for dette dokument. ETCS komponenterne vil ikke blive beskrevet detaljeret i dette dokument, men vil være at finde i [SUBSET-035]. Danske ATC komponenter vil blive omtalt på et overordnet niveau.

Som det ses i ovenstående figur er DK-STM, ligesom ZUB123, forbundet direkte til bremser, traktion og de serielle ATC-komponenter. Isolation Switch er ETCS-navnet for overstropningskontakt, som bruges til at inaktivere DK-STM.

Bremser- og traktionskommandoer sendes samtidig til ETCS gennem PROFIBUS-forbindelsen.

Lokomotivførerens betjening af DK-STM sker via DMI. DK-STM har kun adgang til DMI når ETCS har givet DK-STM overvågningsansvaret.

DK-STM får odometerdata fra ETCS.

Samtidig med at DK-STM sender data til havarilog, sendes disse også til ETCS's JRU.

Definitioner

2v2	2 af 2 system – der beregnes to resultater, som sammenlignes
ATC	Automatisk Togkontrol
CRC	Cyklisk redundanscheck
DA	Data Avaible. En tilstand I DK-STM, hvor den har ansvaret for togkørslen
DK-STM	STM dedikeret til den danske infrastruktur.
DMI	Driver Machine Interface
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FA	Failure. En tilstand i DK-STM, hvor den skal genstartes, før den kan virke igen. ETCS Onboard har ansvaret for togkørslen
FDL	Field Data Link (PROFIBUS)
FFFIS	Form-Fit Functional Interface Specification
HS	Hot Standby. En tilstand I DK-STM, hvor den er klar til at overtage ansvaret for togkørslen. ATC togantennerne er aktive
JRU	Juridical Recording Unit
RBC	Radio Blok Center
RKFS	Processorkort frigivelsessignal
SIL4	Safety Integrity Level 4
SIMIS	Siemens Microprocessor Interlocking System
STM	Specific Transmission Module
TCC	Train Control Computer
TPR	Telegrambit, der angiver position af bæger (har værdien 0 eller 1)

1.3 Referencer

[CodingStandard]	C++ Coding Standard SIMIS® Basissystem DIS: A6Z08110524931/PM2/000/D
[CppStyleGuide]	C++ Coding Style Guide STM-DK G81001-X3107-R005-*
[EN 50128]	CENELEC Standard EN 50128: Railway applications - Software for railway control and protection systems, March 2001
[EN 50129]	CENELEC Standard EN 50129: Railway applications - Safety related electronic systems for signalling, February 2003
[GUT-CodingStandard]	Inspektionsbericht zur sicherheitstechnischen Begutachtung C++ Coding Standard DIS: A6Z00001462993/PM1/000/A
[IN656V1711]	Protokol for seriel kommunikation mellem ATC, TC, MSR3 og Havarilog, Version 3, 1. November 1998
[PEACC+]	Quality Assurance Plan G81001-X3107-U001-*
[SUBSET-035]	Specific Transmission Module FFFIS
[SUBSET-056]	FFFIS STM Safe Time Layer
[SUBSET-057]	FFFIS STM Safe Link Layer
[SUBSET-058]	FFFIS STM Application Layer

1.4 Dokumentlog

00.01	31.03.2011	Første udgave, klar til review	BBE
01.00	01.06.2011	Første udgave	BBE
01.01	30.12.2011	Opdateret efter BDK kommentarer	STN
02.00	19.11.2014	Baseline 3.0 opdatering	BBE

2 Generelt design

2.1 Forudsætning og begrænsninger

DK-STM er en Gateway løsning, hvilket vil sige, at eksisterende funktionalitet fra den oprindelige danske ATC hoveddatamat ZUB123 kan genanvendes. Gateway'en er bindeledet mellem ETCS og ATC systemerne. Kildekoden fra ZUB123 Hoveddatamaten bliver importeret til den nye DK-STM platform, hvor det skal samarbejde med den nyudviklede Gataway komponent som to selvstændige programmer, der udveksler oplysninger.

2.2 Version 2.3.0.d og Baseline 3.0

I april 2008 udkom European Railway Agency med ETCS SRS version 2.3.0d. ETCS SRS Baseline 3.0 udkommer i 2012.

Når DK-STM har fundet en kompatibel ETCS Onboard version, registreres dette i DK-STM, hvorefter denne benyttes ved opstart. Herefter wil ændring af ETCS Onboard version kræve indgreb af en tekniker.

Findes der ingen kompatibel version, skifter DK-STM til FA-tilstanden (Failure).

2.3 Systembeskrivelse

DK-STM indgår som komponent i et samlet ETCS Onboard system, hvor DK-STMs primære opgave er at overvåge et køretøjs færden på de nationale ATC udrustede strækninger vha. informationer fra den nationale infrastruktur. DK-STMs primære funktioner er:

- Læse og afkode data fra den eksisterende infrastruktur via baliser og linjeleder
- Overvåge korrektheden af data og udløse alarm, hvis data er ukorrekte eller ufuldstændige
- Overvåge at køretøjets færden harmonerer med informationer fra infrastrukturen
- Informere lokomotivføreren med aktuel kørselsstatus via DMI
- Modtage interaktion fra lokomotivfører via DMI

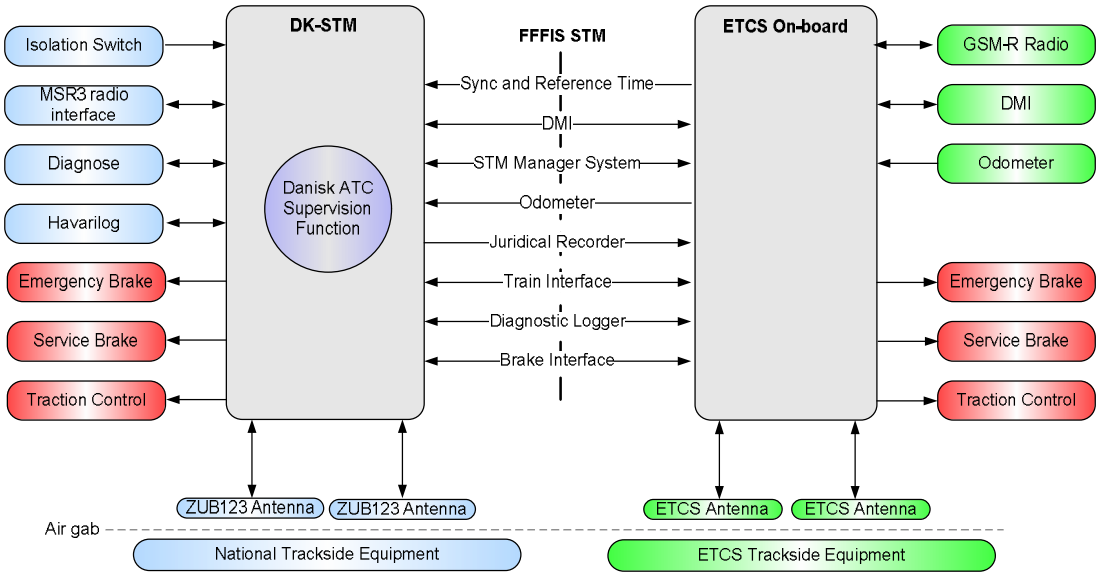
Figur 2 viser et blokdiagram af de komponenter, som indgår i en dansk/national DK-STM konfiguration. De blå komponenter stammer fra det eksisterende ATC system, mens de grønne er ETCS komponenter.

Nødbremse, driftsbremse og traktion styres af både DK-STM og ETCS Onboard (eller andre STM'er for andre lande) – disse er markeret med rødt. Toget er ikke dobbeltudrustet med disse togkomponenter, men deles om disse. Det er ubetinget ETCS Onboard, som bestemmer, hvem der har rådighedsretten over bremserne og traktion.

DK-STM er forbundet til ETCS Onboard via en PROFIBUS forbindelse. Logisk er PROFIBUS-forbindelsen underopdelt i funktioner, der varetager kommunikationen

med ETCS Onboard's periferienheder såsom DMI, Odometer, JRU o.s.v. Specifikationen for forbindelsen er beskrevet på applikationsniveau i [SUBSET-058].

DK-STM varetager funktionaliteten til de eksisterende ATC komponenter.
Isolation Switch, også kaldet overstropningskontakt, bruges i forbindelse med overstropning af nødbremen (driftsbremsen kræver ingen overstropning).
De serielle interfaces MSR3 og Havarilog bruges som i det eksisterende ATC system, hvis de er tilvalgt i DK-STM's vedligeholdelsesvindue – specifikationer hertil kan findes i [IN656V1711]. DK-STM skal ikke benytte TC (Tog Computer) og er derfor ikke udstyret med et TC interface.
Udveksling af strækningsinformationer på strækninger med ZUB123 baliser og evt. tilhørende linjeledere foregår som i det eksisterende ATC system med ZUB123 antenner.
ATC førerrumssignalet og det daværende odometer er erstattet med henholdsvis en standardiseret ETCS DMI og et ETCS odometer, som DK-STM udveksler data med over PROFIBUS'en



Figur 2: Blokdiagram af komponenter der indgår i dansk STM konfiguration

2.3.1 Det samlede ETCS system med DK-STM

ETCS er specificeret i forskellige niveauer – ETCS Levels. Niveauerne afspejler kompleksiteten af systemerne. Der findes på nuværende tidspunkt følgende niveauer:

- ETCS Level 0
- ETCS Level 1
- ETCS Level 2
- ETCS Level 3
- ETCS Level STM

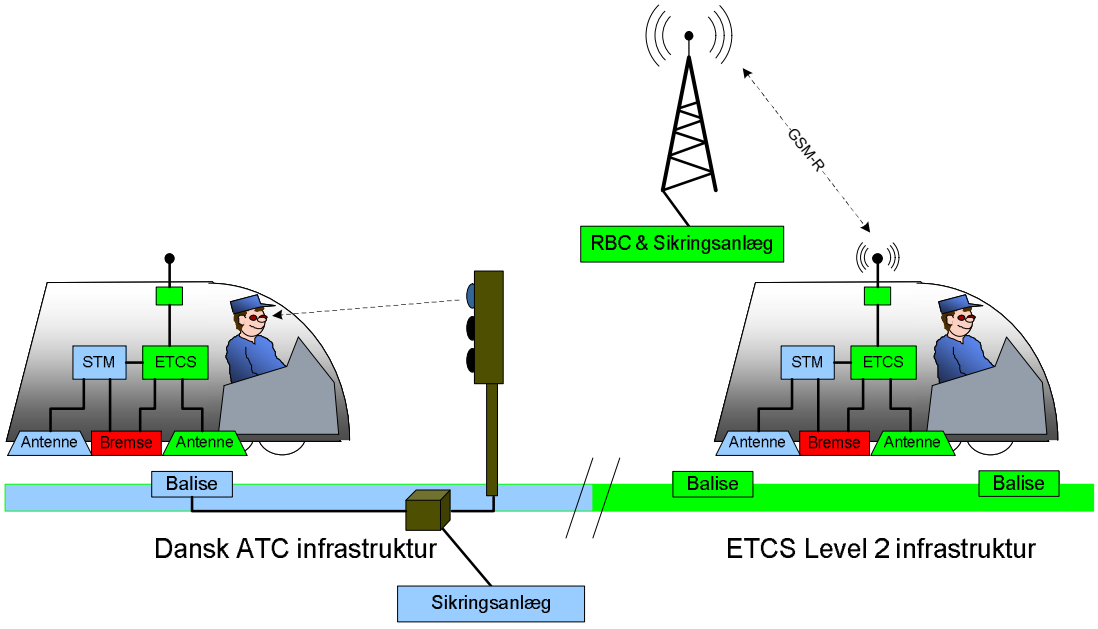
I ETCS Level 0 overvåger ETCS Onboard kun at hastigheden ikke overstiger den indtastede maximum hastighed for toget eller opgivne maximum hastighed for strækningen.

Ved ETCS Level 1 til 3 er infrastrukturen fuldt udrustet med ETCS strækningsudstyr, hvorimod der ved ETCS Level STM benyttes den oprindelige nationale udrustning.

I Danmark er ETCS Level 2 valgt som det system, som skal afløse det danske ATC System. I Figur 3 er der vist, hvorledes kørsel vil foregå henholdsvis for strækninger udrustet med ATC og ETCS systemer. Eftersom begge systemer er afhængige af et spordetekteringssystem (akseltællere eller sporisolationer), er disse ikke medtaget på skitsen.

Komponenter tilhørende ETCS er farvet grønne og de blå farvede komponenter er en del af det danske ATC.

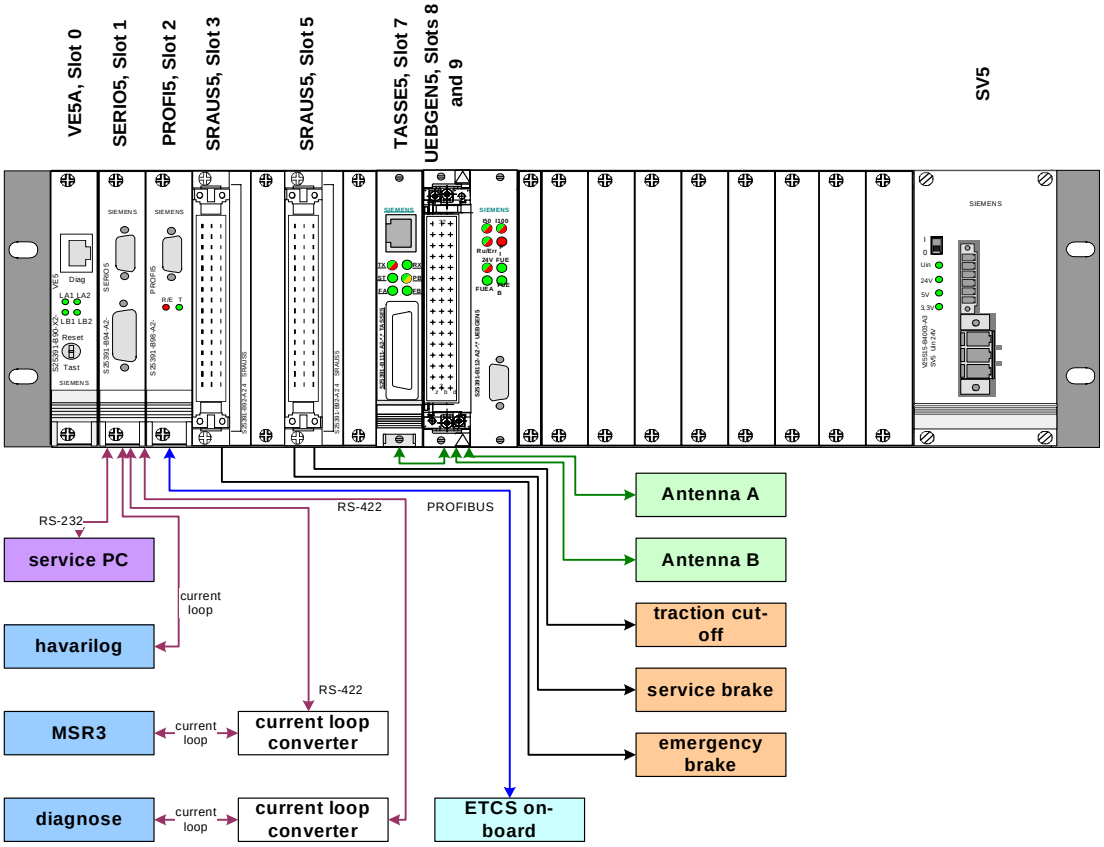
Begge systemer er baseret på antenner og baliser. Baliserne sender via antennerne strækningsinformation til togets overvågningscomputer. I ATC systemet sendes mange forskellige strækningsinformationer, hvorudfra DK-STM kan beregne en bremsekurve. I ETCS Level 2 er baliserne simplificeret – de bruges kun til bestemmelse af position og kørselsretning. Resterende strækningsinformationer bliver transmitteret vha. et GSM-R netværk, som forbinder togene med sikringsanlæggene. I overgangen fra et traditionelt signalsystem til et ETCS Level 2 system kan størstedelen af de optiske signaler udelades.



Figur 3: Dansk ATC og ETCS Level 2

2.4 DK-STM Hardware

DK-STM er hardwaremæssigt opbygget af komponenter fra SIMIS® TCC familien. Figur 2.1 viser skematisk opbygningen af en DK-STM i et 19" rack.



Figur 4: Skematisk opbygning af en DK-STM

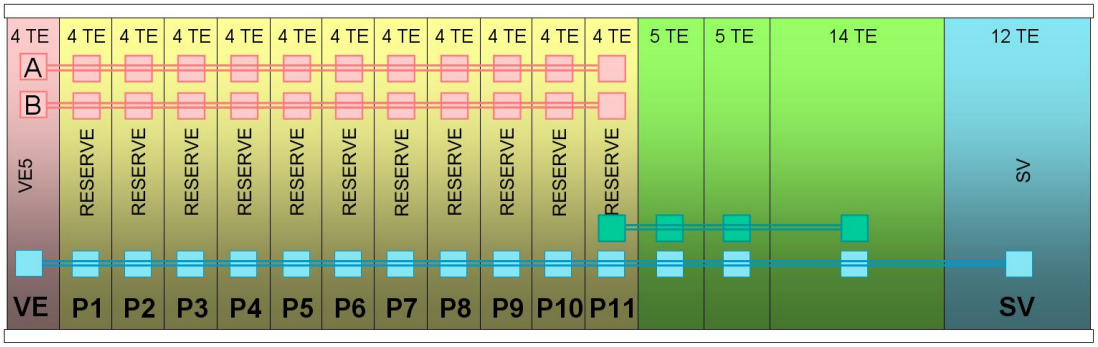
Slot.	Komponent	Anvendelse
0	SIMIS TCC VE5, CPU	DK-STM SW Kommunikation med øvrige komponenter
1	SIMIS TCC SERIO5	Kommunikation med, Havarilog, MSR3 og Diagnose
2	SIMIS TCC PROFI5	Kommunikation med ETCS-Onboard
3	SIMIS TCC SRAUS5	Kommunikation med nødbremse
5	SIMIS TCC SRAUS5	Kommunikation med driftsbremse og traction cutoff
7	SIMIS TCC TASSE5	Lagring af ATC antenne telegrammer og styring af sende/modtage omskiftning
8	SIMIS TCC ÜBGEN5	Kommunikation med eksisterende ATC antenner
19	SIMIS TCC SV5	Strømforsyning

Tabel 2.1: Konfiguration af grundrammen i DK-STM

TCC basissystemet er et 2-kanals computer system (2v2), som er udviklet til sikkerhedskritiske jernbaneapplikationer, der skal leve op til sikkerhedsniveauet SIL4.

2.4.1 SIMIS TCC Grundramme

Grundrammen eller 19" rack'et er opbygget for at opnå stor fleksibilitet. Foruden processorkort og strømforsyning er det muligt at bestykke grundrammen med op til 11 periferikort efter eget valg, plus nogle dedikerede kort til håndtering af forskellige balise systemer.



Figur 5: SIMIS TCC Grundramme

Grundrammen har en bredde på 84 TE (breddeenhed = 5,08 mm) og fordelt som på Figur 5. Højden er 3 HE (højdeenhed = 44,45 mm).

En sikker bus (2-kanal) forbinder CPU kortet med de 11 periferikortpladser. Busserne bruges som sikker kobling af periferienhederne med CPU kortet.

Alle kortpladser bliver forsynet af strømforsyningen, der er monteret på pladsen, som bruger de sidste 12 TE. Derudover er en bus forbundet mellem den 11. periferikortplads og tre ekstra udvidelsespladser, som ikke har forbindelse til den sikre bus.

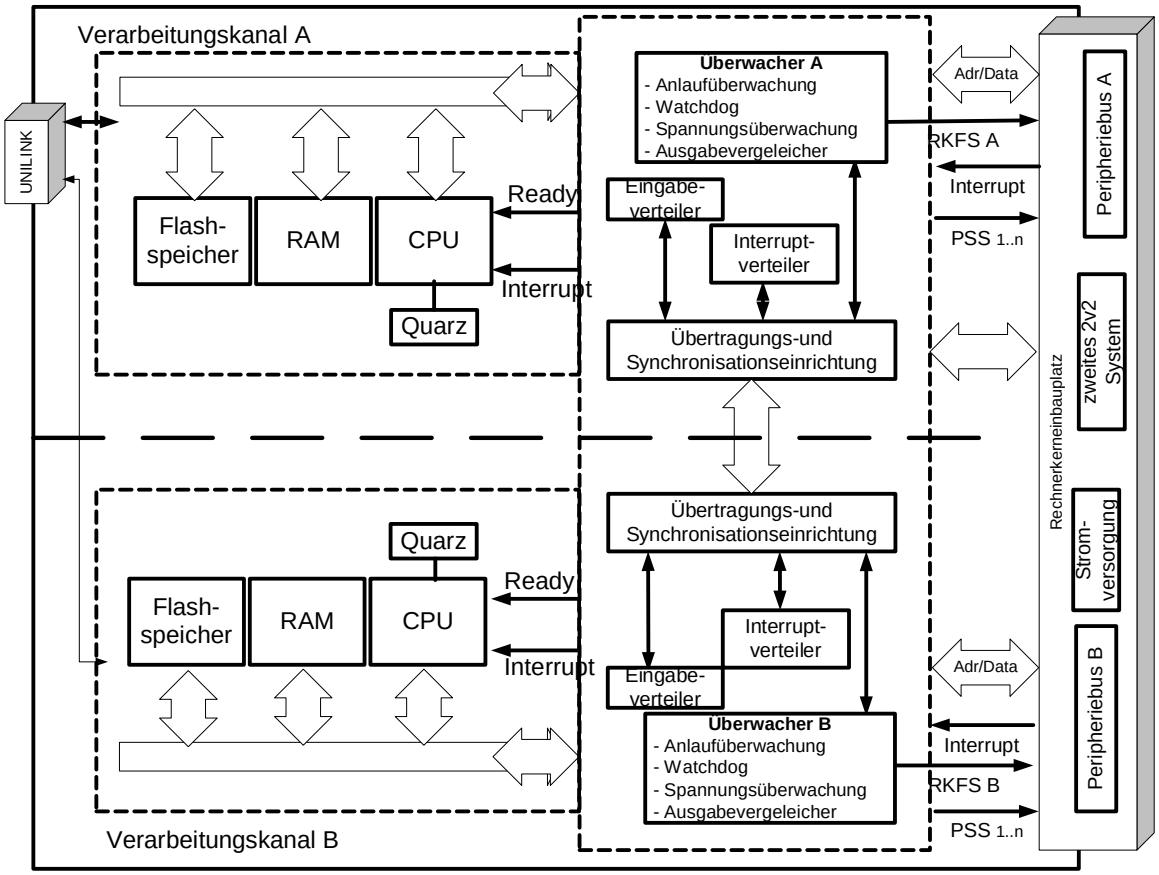
Standardbredden for et periferikort er 4 TE. SRAUS5 kortet er for eksempel 5 TE bredt og vil dermed optage to periferikortpladser.

2.4.2 SIMIS TCC VE5, CPU

VE5 processorkortet er baseret på to 80486DX CPU'er fra AMD, som hver udgør en CPU-kanal. Disse bliver overvåget af et kredsløb, der sammenligner CPU'ernes resultater. I tilfælde af uoverensstemmelse mellem de to CPU'er vil dette medføre CPU-stop, hvilket betyder at alle periferikortene kommanderes til deres sikre tilstand.

Kortet er bestykket med 8 Mbyte flash ram (FRAM) og 2 Mbyte statisk ram (SRAM).

Programmering af kortet foregår via en Unilink-boks, som forbindes til kortet med et RJ45 Ethernet stik og tilsluttes PC'en med et USB stik.



Figur 6: SIMIS TCC VE5 CPU Blokdiagram

2.4.3 SIMIS TCC SERIO5

SERIO5 kortet er udstyret med 5 serielle kanaler. Disse kan konfigureres som RS232, RS422 eller som 20 mA strømsløjfe.

- 2 RS232/RS422 (op til 19,2 kbps)
- 1 RS422/Strømsløjfe (op til 19,2 kbps)
- 1 RS422 (op til 19,2 kbps)
- 1 RS232/RS422 (op til 115,2 kbps)

Desuden har SERIO5 kortet også en indbygget en RTC (Real Time Clock) med batteri-backup og 128kBytes flash ram (FRAM).

2.4.4 SIMIS TCC PROFI5

PROFI5 kortet tilbyder et PROFIBUS FDL (RS-485) interface, ifølge standarden [EN 50170].

2.4.5 SIMIS TCC SRAUS5

SRAUS står for ”sikre relæ udgange”.

SRAUS fås i 2 udgaver. En udgave til 24V, og en udgave til 110V forsyning.

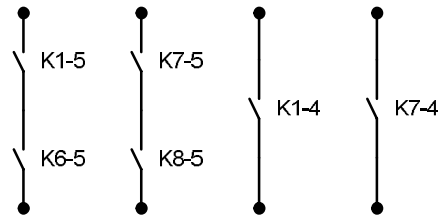
Kortet er monteret med relæer, som er galvanisk adskilt fra den sikre periferibus vha. optokoblere. Relæerne fødes dels af den interne 24V spændingsforsyning, som er galvanisk adskilt fra den eksterne forsyning eller fra den eksterne forsyning, der bruges til at aktivere Isolation Switch’en (beskyttet med en 160 mA sikring).

SRAUS5 er monteret med følgende:

- 2 sikre relæudgange (2 serielle sluttekontakter)
- 2 normale relæudgange (enkelt sluttekontakt)
- 1 sikker overstropningsindgang (2 relæspoler)
- 3 sikre overstropningsrelæudgange (2 serielle sluttekontakter)
- 2 normale overstropningsrelæudgange (enkelt sluttekontakt)
- 2 normale overstropningsrelæudgange (enkelt brydekontakt)

De benyttede relæer hedder SR6B4018/SR6B4024 og kommer fra producenten Schrack. Relæerne er af typen ’tvangsstyrede relæer’ efter normen EN50205.

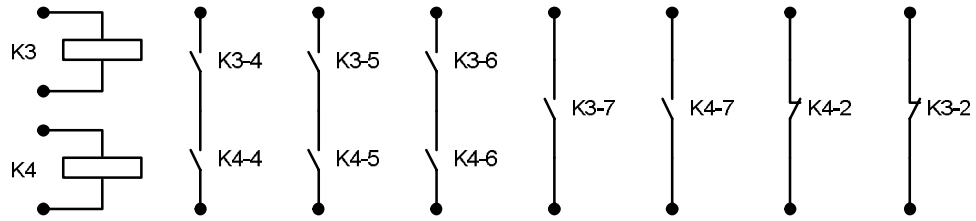
Figur 7 viser de 2 sikre relæudgange og de 2 normale relæudgange. Relæerne K1, K6, K7, K8 styres via softwaren. Relæernes tilstand udlæses på begge kanaler fra to uafhængige målepunkter. De sorte prikker symboliserer hver især et ben på stikket, som er monteret på forsiden af SRAUS5 kortet.



I

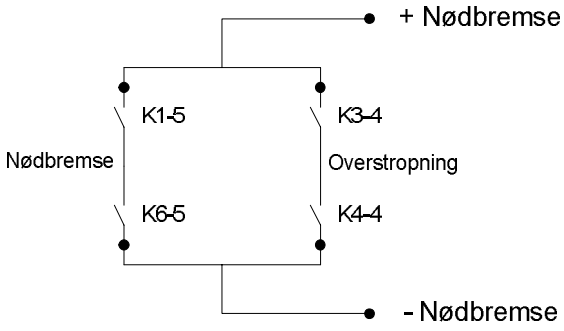
Figur 7: Diagram af sikre/normale relæudgange

I Figur 8 ses de to relæer og deres kontaktsæt, der udgør det sikre overstropningskredsløb. Relæer K3 og K4 skal aktiveres med 24V/110V.



Figur 8: Diagram af overstropningsrelæer og deres kontaktsæt

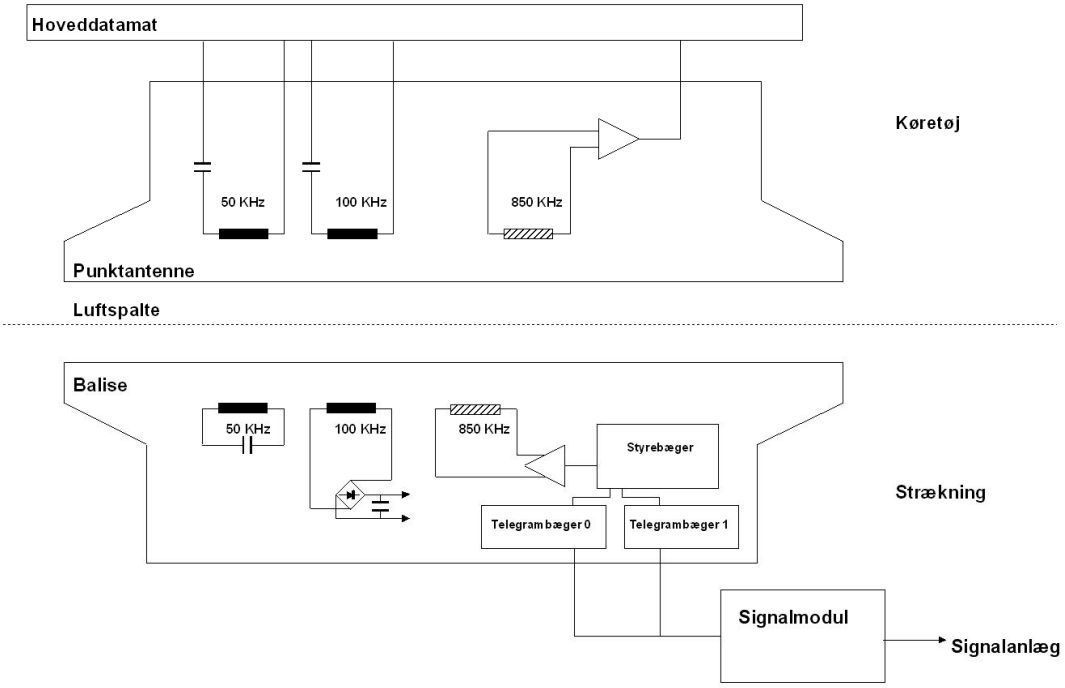
Overstropningsrelæerne kan bruges i en fejlsituation, hvor nødbremsen er aktiveret (et af bremserelæerne ikke er trukket), samtidig med, at der ønskes at toget skal bugseres. Overstropningsudgangene skal forbindes parallelt med nødbremserelæudgangene som vist i Figur 9. For at gennemføre en overstropning, skal både relæerne K3 og K4 aktiveres, således at der opnås gennemgang/kortslutning mellem "+ Nødbremse" og "- Nødbremse".



Figur 9: Diagram af enkelt nødbremsekredsløb

2.4.6 SIMIS TCC TASSE5

TASSE5 kortet danner sammen med ÜBGEN5 et integreret interface til ZUB punktantennen.
TASSE er en forkortelse af "**T**elegramm-**A**ufzeichnungs-Bausgruppe mit FIFO-**S**peicher und **S**ende/**E**mpfangsumschaltung" og bruges til at modtage og afkode telegrammer fra 850 kHz datakanalen.



Figur 10: Skitse af punktantenne og balise

Figur 10 viser en skitse af kredsløbene, som bruges til kommunikation over luftspalten mellem togantennen og balisen. Øverst ses antennen, som er monteret på køretøjet og nederst balisen, der styres fra signalanlægget.

Detekteringskredsløbet (50 kHz) overvåger om antennen er placeret over en balise.

Energikanalen(100 kHz) føder balisen med induktivt overført energi.

Datakanalen (850 kHz) bruges til overførelse af balisedata fra telegrambægerne til togantennen.

Baliserne får tilført induktivt overført energi ved hjælp af et serieresonanskredsløb, der er afstemt til 100 kHz.

Energien fra de 100 kHz akkumuleres i en kondensator. Når kondensatoren opnår en spænding på 18 volt kobles elektronikken i styrebægeret ind.

Indgangskoden (2 af 6 kode) aftastes fra signalmodul eller fastkodet stik. Indgangskoden bruges til at udvælge et telegram i hver af de to telegrambæger.

De maksimalt 120 bit (96 databit) lange telegrammer transmitteres serielt over til FM-modulatoren, som sender disse FM-moduleret omkring bærefrekvensen 849 kHz (823,5/875 kHz), 50 kBaud.

En korrekt balisepassage kræver detektering af balise samt mindst 3 telegrammer med identiske nyttedata (telegram data eksklusiv. TPR og CRC bits).

2.4.7 SIMIS TCC ÜBGEN5

ÜBGEN står for ”Overvåget Generator”. Dette kort har til hovedformål at detektere baliser og overføre energi til disse.

Balisedetekteringskredsløbet bruges udelukkende til overvågning af, om en balise passeres. Balisedetekteringskredsløbet er en passiv resonanskreds afstemt til 50 kHz. Resonanskredsens selvinduktion er viklet på en ferritstav, som udgør antennen. Passerer køretøjets punktantenne hen over balisen, vil der ske en strømsænkning i punktantennens 50 kHz kredsløb, fordi resonanskredsen forstemmes.

2.4.8 SIMIS TCC SV5

SV5 er TCC systemets strømforsyningskort. Kortet fås i 2 udgaver. En 24V og en 110V. Kortene er funktionsmæssig ens og adskiller sig kun ved indgangsspændingen:

- 24V/110V, maks. belastning 4,2A
- 5 V, maks. belastning 1,0A
- 3,3 V, maks. belastning 4,6A

Kort	Effektforbrug, typisk
VE5	2,7 W
SERIO5	3,5 W
PROFI5	2,3 W
SRAUS5	13 W (6,5 W * 2)
TASSE5	21,7 W
ÜBGEN5	5,6 W
SV5	10,0 W (virkningsgrad ca. 83%, 48,8 W)
Samlet	58,8 W

SV5 kortet skal forsynes af en 24V/110V forsyning med en rippelspænding, der er mindre end 2%.

Ved overspænding (indgangsspænding større end 35V/159,5V), bliver en sikring udløst.

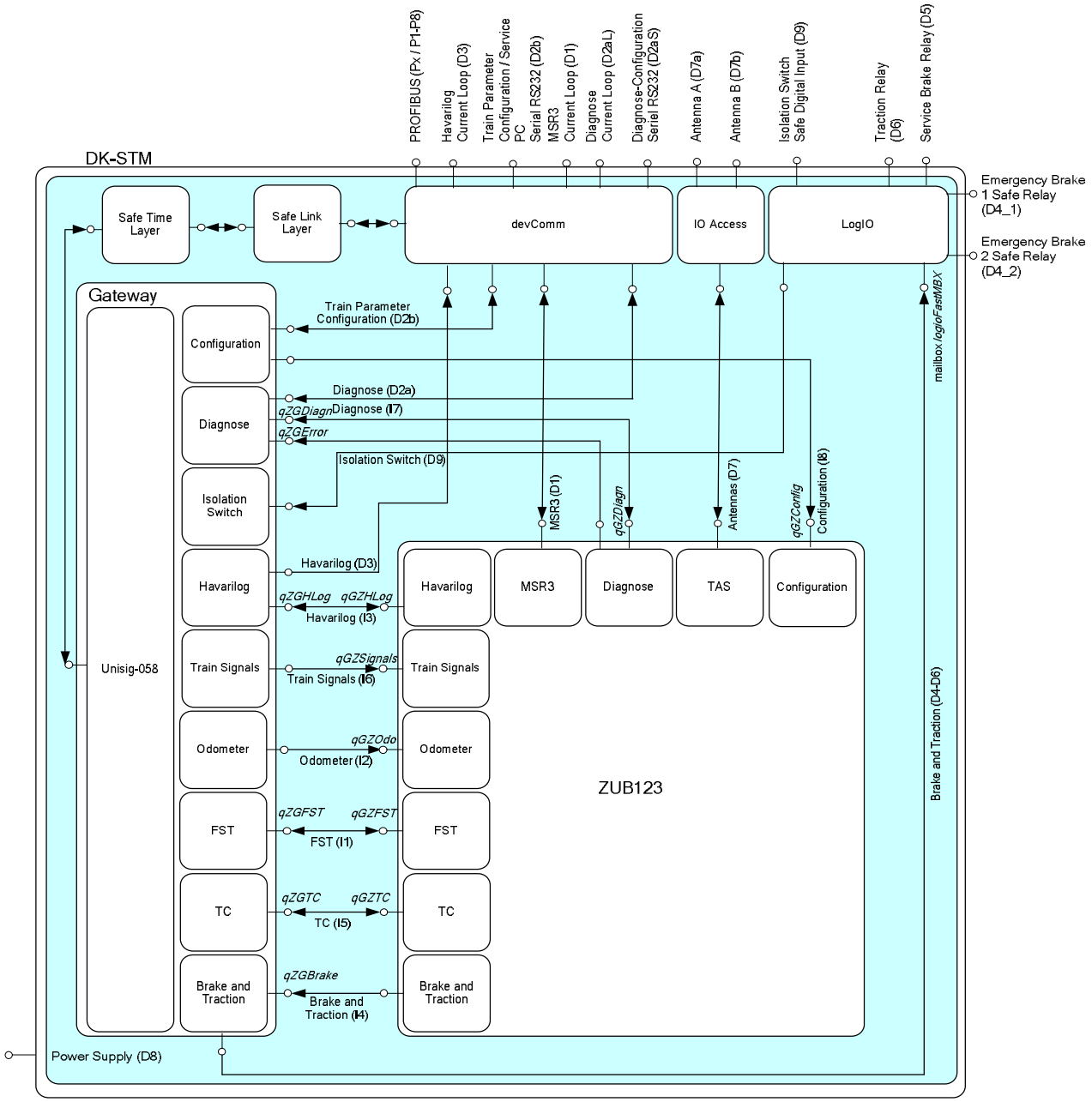
Ved underspænding (indgangsspænding mindre end 14V/41,9V), vil SV5’eren software-mæssigt frakoble.

2.5 DK-STM software

DK-STM softwaren består hovedsageligt af to bestanddele – den importerede del fra ATC hoveddatamaten, som varetager den trafikale proces, samt en Gateway del, der i hovedtræk laver en konvertering mellem ETCS og ATC systemerne.

Figur 11 viser den logiske opdeling af DK-STM. Yderst på diagrammet ses forbindelserne til omverdenen. De er forbundet til nogle drivere, som bliver benyttet til at kommunikere med hardware'en. Softwaredelene er i figuren forbundet med streger med pile, som angiver senderetningen af data.

De to software komponenter Gateway og ZUB123 er implementeret som to selvstændige tasks, der afvikles på sandtids operativsystemet CPM32.



Figur 11: Overordnet software diagram

2.5.1 ZUB123, den trafikale proces

Den trafikale proces er den software, som findes i den eksisterende ATC hoveddatamat. Der er ikke ændret i den funktionsmæssige del af komponenten – kun interfaces er ændret, så man sikrer at den trafikale proces forbliver intakt.

Denne komponent er programmeret i Pascal og arbejder i et selvstændigt task. Kommunikation med Gateway delen foregår vha. køer (datakanal). Anden kommunikation foregår gennem drivere.

Den trafikale proces har følgende funktioner:

- Evaluere og handle på baggrund af modtaget baliseinformation
- Beregne bremsekurve hvert 200 ms
- Beregne og overvåge den aktuelle hastighed
- Sende ZUB123 diagnose data
- Sende ZUB123 havarilog data
- Udveksle data over MSR3 Radio
- Sende bremse/traktion information til Gateway
- Sende ZUB123 tilstandsinformation til Gateway via FST
- Modtage kommandoer fra Gateway via FST

Styring af de trafikale funktioner sker gennem ETCS's tilsluttede DMI, f.eks "rangering" og "passage stop". Indikationer fra de trafikale funktioner vises ligeledes på DMI, f.eks. "Løs ATC" og "Nød Brems".

2.5.2 Gateway

Gateway delen, er den ny SIL4 udviklede komponent, som har til formål at være bindeled mellem ETCS Onboard og den trafikale proces.

Gateway komponenten består af en generisk del, som i korte træk håndterer udveksling af STM pakker mod ETCS Onboard – disse er specificeret i [SUBSET-058]. Derudover udgør den generiske del også den logiske tilstandsmaskine, som er beskrevet i 3.3 Driftstilstande for DK-STM.

Det er valgt at adskille den generiske del og den nationale del i Gateway komponenten for at opnå et design, hvor kravene til henholdsvis ETCS og BaneDanmark kan holdes adskilt. Den nationale del, som hovedsageligt skal sørge for at kommunikationen med ZUB123 komponenten og tilgår de generiske funktionaliteter.

Gateway'ens funktioner mod ZUB123 task'et er følgende:

- Konfigurere ZUB123 og starte ZUB123 task
- Sætte DK-STM i FA., hvis Isolation Switch er aktiveret
- Konvertere ETCS Onboard odometer data til odometer pulser (svarende til den forhenværende impulse giver)
- Sende kabinedata til ZUB123 vha. Train Signals
- Overføre togdata til ZUB123 vha. TC interface
- Aflæse position fra sidst passeret balise vha. TC interface
- Styre ZUB123's overvågningstilstand vha. FST interface
- Aflæse ZUB123's informationer vha. FST interface
- Aflæse ZUB123's bremsestatus og afh. af situationen aktivere bremsen.

- Sende diagnose og havarilog data videre.

Gateway'ens funktioner mod ETCS Onboard er følgende:

- Udveksle DMI informationer – styring af brugerinterface
- Modtage odometer data
- Sende diagnose og havarilog data
- Sende nødbremse-, driftsbremse- og traktionskommandoer

2.5.3 Drivere

Driverne er den software, som gør det mulige at komnunikere med periferiudstyr.

2.5.3.1 DevComm

DevComm er den driver, der bruges til periferikort med seriel kommunikation.

2.5.3.2 IO Accsses

IO Access er et interface som blandt andet tilbyder:

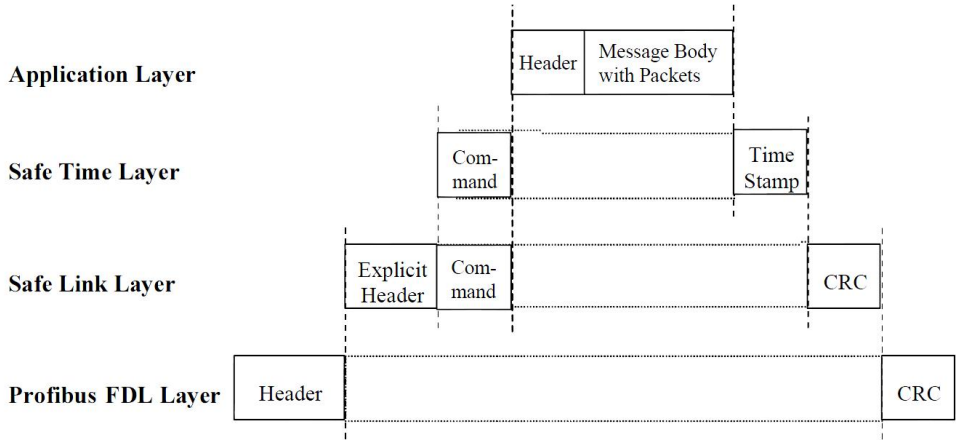
- Port-orienteret adgang til hardwaren
- Signalering ved tilstandsændring
- Bearbejdning af interrupt

2.5.3.3 LogIO

LogIO er et task, som bruges i forbindelse med bit-vise læse/skrive operationer med periferiudstyr. Det sørger automatisk for at opdatere brugeren af en bestemt bit på et periferikort, hvis dette ændrer tilstand. Dette bruges f.eks. med SRAUS5 kortet, hvor man ønsker at sætte/læse enkelte relæers tilstand.

2.5.3.4 Safe Link Layer & Safe Time Layer

PROFI5 kortet arbejder på PROFIBUS FDL niveau. For at Gateway software'en på applikationsniveau kan kommunikere med ETCS, er der brug for to mellemliggende lag, som kaldes SafeTime Layer og Safe Link Layer. Disse er specificeret i henholdsvis [SUBSET-056] og [SUBSET-057].



Figur 12, PROFIBUS, STM FFFIS lag-opdeling

3 DK-STMs hovedfunktioner

3.1 DK-STMs rolle i det samlede ETCS system

DK-STM skal bruges i overgangsfasen, hvor ETCS infrastrukturen bliver implementeret. I denne overgangsfase vil strækningerne have forskellige togkontrolsystemer. Nogle vil være udstyret med dansk ATC mens andre vil være udstyret med ETCS.

På de strækninger, som endnu ikke har fået udskiftet dansk ATC med ETCS udstyr, indgår DK-STM i ETCS Onboard delen til at overvåge dansk ATC kørsel samt kommunikere med ETCS Onboard systemet.

Det gamle og velkendte ATC Førerrumssignal erstattes af den nye ETCS betjeningsflade (DMI). ETCS og DK-STM kan dermed betjenes vha. samme betjeningsenhed.

3.2 Kørsel med ETCS

3.2.1 Kørsel med ETCS på ETCS udrustede strækninger

Strækningen er udstyret med Euro Baliser, som virker som kilometersten – deres formål er alene at give en stedbeskrivelse og fastsætte bevægelsesretningen.

De ydre signaler benyttes ikke. Kørselstilladelse (MA, Movement Authority) sendes via Euro Radio/GSM-R fra RBC (Radio Block Center) til ETCS Onboard.

ETCS Onboard har det totale ansvar for overvågningen og bremsning ved faresituationer. Der vil løbende blive beregnet bremsekurver ud fra modtagne informationer fra Euro Baliser og Euro Radioen.

DK-STM er i dvaletilstand, hvilket vil sige, at ATC togantennerne ikke er aktive og at evt. danske ATC Baliser ignoreres.

3.2.2 Kørsel med ETCS på ikke ETCS udrustede strækninger (DK-STM)

ETCS Onboard har videregivet overvågnings- samt bremseansvaret til DK-STM.

DK-STM benytter det eksisterende ATC strækningsudstyr til evt. beregning af bremsekurver. Med DK-STM som overvågningsansvarlig er det muligt at bruge samtlige kørselsmønstre, som er tilgængelig i dansk ATC – disse er nedenfor listet.

ATC kørselsmønstre:

- Kørsel under normale forhold på strækninger med faste ATC-anlæg
  - Kørsel med ATC-overvågning
  - Kørsel ud af station
  - Forsignalering
  - Kørsel ind på station
  - Hastighedsnedsættelser
  - Stop og ryk frem
  - Automatisk sikrede overkørsler

I

- Kørsel under normale forhold på strækninger med faste ATC-togstopanlæg
  - Kørsel med ATC-togstop
  - Kørsel ud af station
  - Forsignalering
  - Kørsel ind på station
  - Hastighedsnedsættelser
  - Stop og ryk frem
  - Automatisk sikrede overkørsler
- Kørsel under normale forhold på strækninger uden faste Togkontrolanlæg
- Rangering
- Kørsel med ATC under uregelmæssigheder
  - Ind-, ud- og forbirangering
  - Skriftlig ud- og forbikørselstilladelse
  - Udkobling af ATC-anlæg
  - Melding
  - Fejl

I denne kørselstilstand er både ETCS og ATC antennerne aktive. ETCS antennen er aktiv fordi det skal være muligt for ETCS Onboard at skifte til anden infrastruktur, hvis toget kører ud fra området med ATC strækningsudstyr (passage af ETCS grænsebalisepar).

3.2.3 Overgang mellem ETCS udrustede og ikke udrustede strækninger.

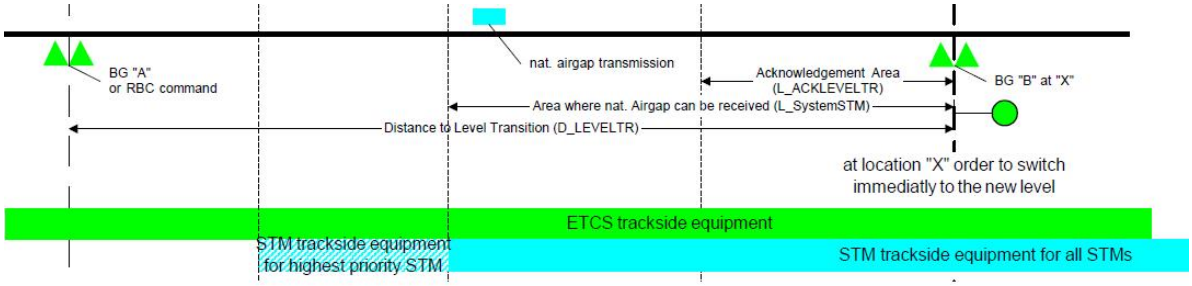
I grænseområdet mellem ETCS og ATC vil den afgrænsede strækning være dobbelt udrustet.

Det normale forløb vil være:

Toget vil først møde en fremskudt ETCS Balise gruppe, som varsler med afstanden til grænsen. ETCS Onboard sætter DK-STM i ”Hot Standby”, hvilket giver DK-STM lov til at aktivere ATC-antennerne.

Senere vil toget passere en ATC Balise med nationale strækningsinformationer, så DK-STM kan beregne en bremsekurve. Det er stadig ETCS Onboard, som har overvågningsansvaret.

Grænsen er markeret med en ETCS grænsebalisegruppe. Ved passering af denne, beordrer ETCS Onboard DK-STM til at gå i tilstand ”Data Available”, som betyder, at DK-STM har overvågningsansvaret.



Figur 13, Eksempel på et grænseområde

3.2.4 Overgang mellem to ikke ETCS udrustede strækninger

Grænseovergangen mellem to STM'er ligner meget overgangen fra ETCS til STM. Grænseområdet vil dog indeholde strækningsudstyr for de to lande, plus ETCS udstyr.

ETCS Onboard er stadig den bestemmende og skifter overvågningsansvaret fra den ene STM til den anden STM, når ETCS grænsebalisegruppen passeres.

3.3 Driftstilstande for DK-STM

DK-STM følger de driftstilstande, som også kaldes for STM States i ETCS verdenen. STM States er fastsat i [SUBSET-035] kapitel 7.3.

Herunder gennemgås de enkelte tilstande ganske kort.

3.3.1 No Power (NP)

DK-STM er ikke tilsluttet forsyningsspænding.

3.3.2 Power On (PO)

Efter at DK-STM er tilsluttet forsyningsspændingen sker overgangen til PO. I PO gennemføres selvtest og synkronisering af PROFIBUS'ens Safe Time Layer. Når dette er opnået, skal DK-STM oprette nødvendige Profibus forbindelser. Så snart disse er forbundet, skal DK-STM anmode om tilladelse til at gå i CO

3.3.3 Configuration (CO)

I tilstanden CO konfigureres DK-STM hovedsageligt med ETCS togdata fra ETCS-Onboard. Efter dataudvekslingen vil DK-STM anmode om tilladelse til at gå i DE.

I DK-STM udveksles følgende parameter:

- Toglængde
- Maks. hastighed

3.3.4 Data Entry (DE)

Tilstanden DE bruges til konfigurere DK-STM med de 4 specifikke togdata. I DK-STM udveksles følgende parameter:

- Toglængde (værdi fra ETCS togdata benyttes. Kan kun ændres ved indtastning af ETCS togdata)

- Bremseprocent
- Maks. Hastighed (værdi fra ETCS togdata benyttes. Kan ændres i DE)
- ATC retning

Værdierne indtastes vha. ETCS DMI.

Tilstanden DE anvendes kun denne ene gang i forbindelse med opstartsproceduren.

Såfremt DK-STM har brug for nye specifikke togdata under STM kørsel, f.eks efter Rangering, kan disse anmodes uden at skulle forbi DE ved at indtaste nye ETCS togdata, hvorefter DK-STM igen anmoder om at få de 4 specifikke togdata.

Når DK-STM'en har fået overført sine specifikke togdata, anmoder den om at gå i CS.

3.3.5 Cold Standby (CS)

I CS er DK-STM initieret, testet og færdig konfigureret. DK-STM har ikke tilladelse til at have aktiverede antenner i CS og kan derfor ikke modtage strækningsinformation fra sporet.

3.3.6 Hot Standby (HS)

I tilstand HS, aktiveres antennerne og DK-STM er nu i stand til at modtage informationer fra baliserne i sporet.

DK-STM er klar til at overtage overvågningen – mangler kun en kommando fra ETCS- Onboard.

3.3.7 Data Available (DA)

DK-STM har overtaget overvågningen og der køres efter de danske ATC regler, hvilket vil sige, at det er muligt at bruge de gamle førerrumssignalsfunktioner via ETCS DMI.

Det er kun i tilstand DA, at DK-STM har rettighed til at bruge bremsen – i alle andre tilstande er det ETCS Onboard, som tager sig af bremsefunktionen. DK-STM har direkte forbindelse til bremsen. DK-STM giver samtidig bremse/traktion-kommandoer til ETCS Onboard.

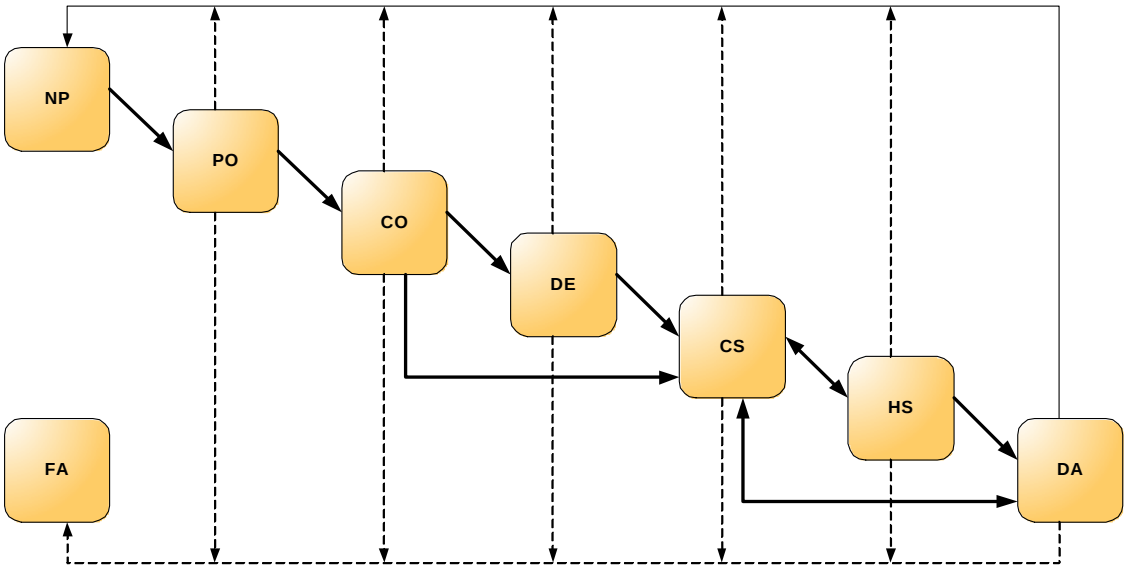
3.3.8 Failure (FA)

Der er sket en uforudset handling i DK-STM. Når DK-STM er gået i tilstand FA, overtager ETCS Onboard overvågningen og en evt. nødbremsning.

Tilstand FA er en "afsluttende" tilstand. Dvs. at DK-STM skal slukkes og startes forfra fra tilstand NP.

3.4 Driftshændelser for DK-STM

De første fire STM tilstande (**NP**, **PO**, **CO** og **DE**) kan kaldes for klargørings- eller oprigningstilstande. Når DK-STM først er oprigget og er i STM tilstand **CS**, vil disse fire tilstande ikke længere kunne tilgås, før at DK-STM har været afbrudt fra spændingsforsyningen.



Figur 14: Mulige STM tilstandsovergange

De tre mest interessante til stande er **CS**, **HS** og **DA**, som kan beskrives med henholdsvis *dvale*, *klar til overvågning* og *overvågning indkoblet*.

Det er udelukkende ETCS Onboard, som bestemmer, hvilken operativ tilstand DK-STM skal befinde sig i. DK-STM har kun bemyndigelse til at gå i tilstand **FA**, hvis der forekommer en uforudset handling eller den virtuelle tilstand **NP**, hvis strømforsyningen udebliver.

3.4.1 Trip kørsel

Ved nødbremsning over en ”transition” fra ZUB123 til ETCS vil ETCS udføre en TRIP-kørsel og fortsætte nedbremsningen til stilstand.

Specielt vil en nødbremse blive indledt, hvis DK-STM er under Rangering og kører over en ”transition”.

4 Sikkerhed

I dette kapitel forklares, hvilke designmæssige hensyn, der er taget for at opnå en hardware/software-løsning, som lever op til SIL4 kravene.

4.1 Hardware

DK-STM er baseret på Siemens SIMIS® TCC Hardware platform, som er designet til sikkerhedskritiske jernbane-applikationer efter specifikationerne givet i [EN 50129] for et SIL4 system.

Hardwaren er ”hyldevare” hos Siemens og er i dag anvendt i en række jernbane applikationer – den teoretiske sikkerhed ved TCC hardware’en er derfor eftervist at være ”proven-in-use”.

Systemet er opbygget efter 2-kanal princippet, 2v2. Processor-kortet VE5, har to processorer som synkroniseres. De afvikler identisk kode, som bliver sammenlignet af et overvågningsmodul. Overvågningsmodulet sørger kontinuert for, at der ikke bliver ageret på hardwarefejl fra en af de to processorkanaler. Diagram over VE5 kan ses i Figur 6.

VE5-kortet er ligeledes forbundet med periferikortene vha. af 2v2 princippet. Begge processerings-kanaler føres ud til periferikortene (Kanal A og Kanal B) med hver en parallelforbundet bus, som består af følgende forbindelser.

8 bit	Adresse/data bus
1 bit	Klok
16 bit	Periferikort vælger
1 bit	Frigivelsessignal (RKFS)
1 bit	Fælles interrupt

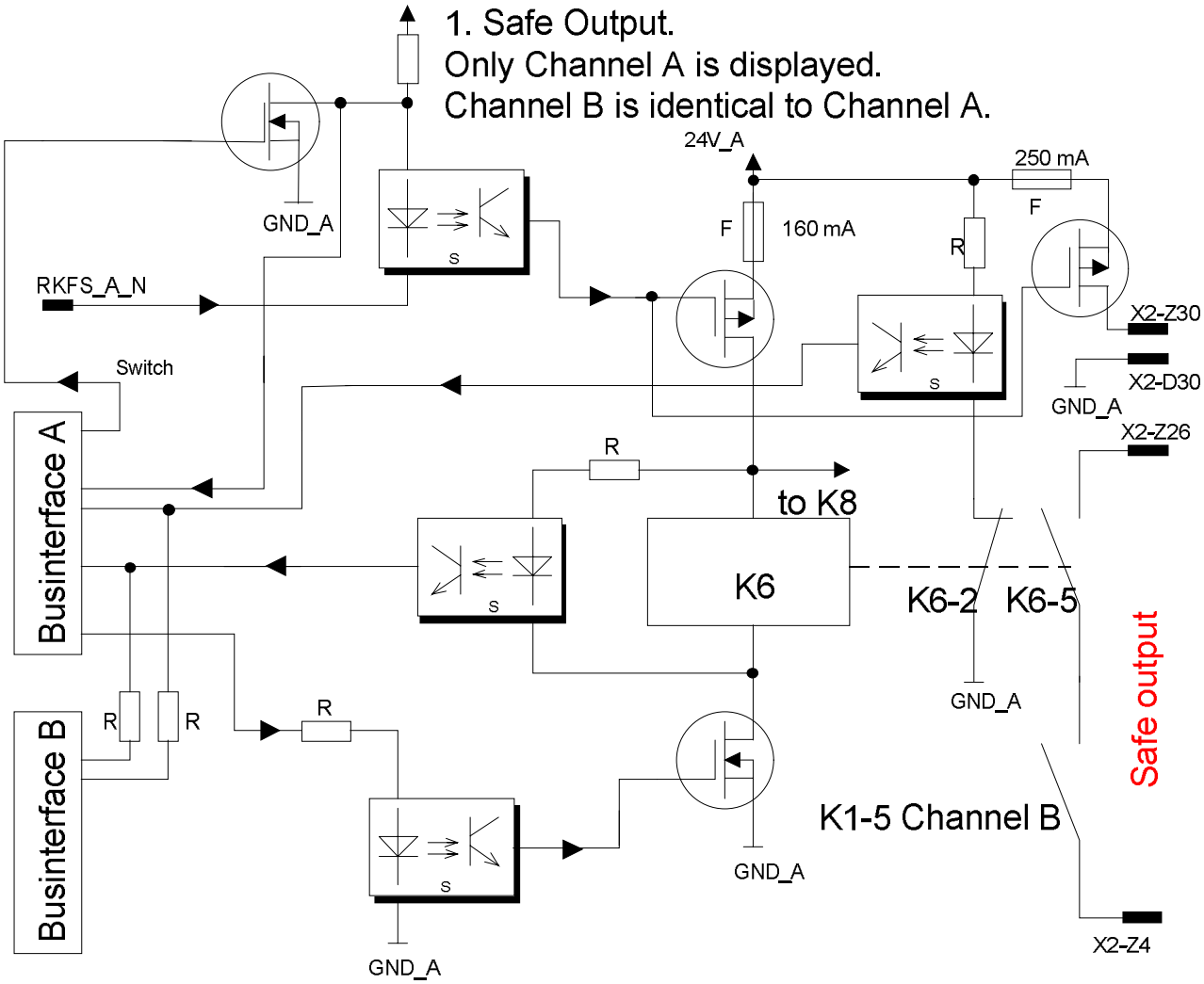
Tabel 1, Bussignaler for en enkelt kanal

Overvågningsmodulet indeholder en watchdog, der holder øje med, at et task ikke overstiger dens pre-definerede eksekveringstid – f.eks hvis CPU’en ikke kan klare belastningen.

Spændingsforsyningen, SV5 bliver også overvåget af VE5 – I tilfælde af dårlig eller udeblivende forsyning, vil dette også medføre en sikker reaktion.

4.1.1 Nødbremse

Nødbremsekredsløbet er opbygget efter princippet, at hvis en relæfejl erkendes på SRAUS5 kortet vil dette medføre en afbrydelse af de kontakter, som er forbundet med bremserne, så disse bliver inaktive og bremser toget. Relæfejl detekteres af et program, der tester relæernes tilstand. I tilfælde af strømafbrydelse vil kontakterne også afbryde og bremse toget – selv hvis et relæ er fastsvejst, vil konstruktionen med serielforbindelsen af to uafhængige relæer give en sikker afbrydelse af bremserne.



Figur 15, Diagram over den ene kanal af en sikker relæudgang.

4.1.1.1 2-kanal system

I Figur 15 ses diagrammet over de komponenter, som udgør den ene af de to kanaler af det sikre bremsekredsløb. Den sikre udgang styres af relæerne K6 (kanal A) og K1 (kanal B – ikke illustreret).

Der er tre betingelser, som skal opfyldes for at trække relæet K6:

- Kortet skal frigives af processorkortet VE5 vha. RKFS-signalet
- Kontakten fra Businterface'et A skal aktiveres
- Signalet fra Businterface'et A, som styrer nederste MOSFET skal aktiveres

Tilstanden af relæ K6 måles fra to uafhængige målesteder. Der måles henholdvis på spændingspotentialet over relæspolen samt tilstanden af brydekontaktsættet K6-2.

Designet med de to uafhængige kanaler følger forskrifterne givet i [EN 50129] D.2.1. for primær uafhængighed.

Sekundær uafhængighed svarende til [EN 50129] D.2.2 opnås med de to uafhængige RKFS signaler fra processorkortet.

4.1.1.2 Cyklisk test

Cykliske test af relæerne, der indgår i de 2 sikre udgange (K1, K6, K7 og K8), vil opfange en defekt (kontaktsæt i uventet stilling) indenfor et sekund. En defekt vil medføre en sikkerhedsafbrydelse.

Fejl på businterface'et til og med styring af relæspoler vil detekteres af cykliske test indenfor en halv time og medføre en sikkerhedsafbrydelse.

4.1.1.3 Galvanisk adskillelse

Galvanisk adskillelse opnås ved brug af optokoblere. Disse er testet med prøvespændingsstød på 1500 V (afstand 2,5 mm).

4.1.1.4 Overstrømsbeskyttelse

Relæspolerne er beskyttet med sikringer på 160 mA – typisk strøm er 90 mA.

4.1.2 Driftsbremse

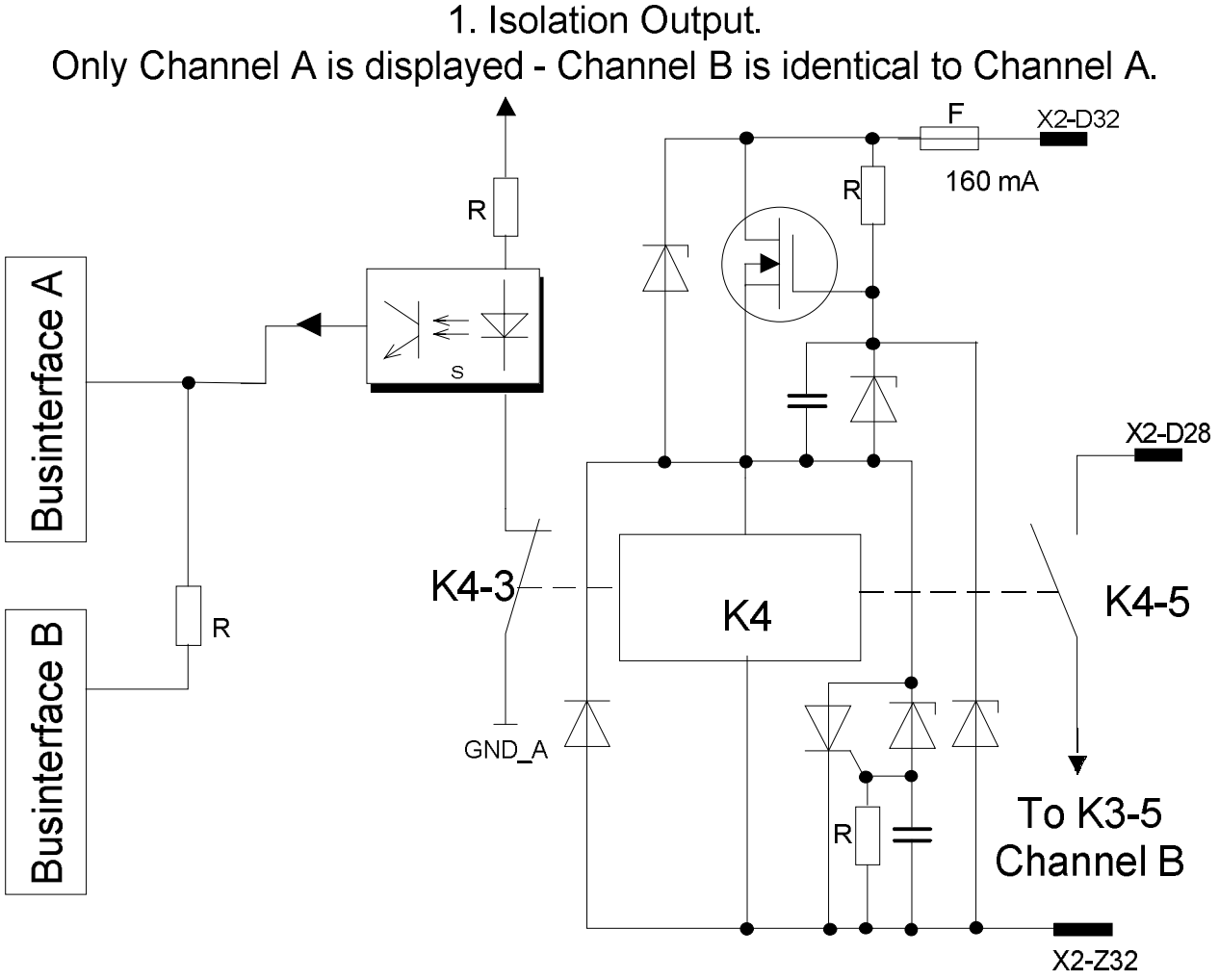
Driftsbremsen benytter ikke en sikret udgang, da den ikke er sikkerhedskritisk.

4.1.3 Overstropning/Isolation Switch

Overstropningskredsløbet for kanal A kanal er vist i Figur 16. Kanal B er opbygget identisk.

Relæspolen K4 skal påvirkes udefra med en spænding på 24 V for at aktivere overstropningen af Kanal A. Ligeledes skal dette gøres for Kanal B (K3) for at lave en kortslutning af de to serieforbundet sluttekontakter (K4-5 og K3-5).

Tilstanden af relæerne udlæses på begge businterfaces for begge kanaler.



Figur 16 Diagram over den ene af de to overstropningskanaler

4.1.4 Traktion

Traktion benytter ikke en sikret udgang, da den ikke er sikkerhedskritisk.

4.1.5 Seriel kommunikation

Seriel kommunikation sikres software-mæssigt vha. checksum. Derudover bliver PROBIBUS'en beskyttet af Safe Link og Safe Time layers.

4.1.6 ZUB123 antenner – luftspalten

Der er i det eksisterende ATC system gjort mange tiltag for at kommunikationen over luftspalten foregår sikkert og pålideligt.

Baliserne er udstyret med to telegrambægre med hver sit TPR bit. TPR angiver positionen af telegrambæger – som enten kan være 0 eller 1.

Modtagelses af balisedata foregår i et serielt 2-kanal system. Balisen sender skiftevis telegrammer fra de to telegrambægre. Nyttedata fra de to telegrambægre skal være identiske – de bliver sammenlignet ved modtagelse.

Hvilket telegram, der skal sendes fra et telegrambæger, vælges vha. en 2 af 6 kode. De to telegrambægre styres af to uafhængige 2 af 6 koder.

En korrekt balisepassage kræver detektering af balise samt mindst 3 telegrammer med identiske nyttedata (telegram data eksklusiv TPR og CRC bits).

Baliserne er koblede med en afstandsparameter, der fortæller, hvornår det kan forventes, at toget skal modtage nye balisedata. Om denne sikring er aktiveret, er en del af telegramdata'ene – det er således muligt at deaktivere denne sikring.

Balisedata er beskyttet af et 8 bit langt CRC.

Justering af antenner må kun foretages af personale med rettigheder hertil – justering foretages via en under-menu i DMI, som er beskyttet med kodeord.

4.2 Software

Softwaren i DK-STM består af tre hovedblokke:

- TCC basis software
- ZUB123 task'et, den trafikale process fra ATC hoveddatamaten
- Gateway task'et

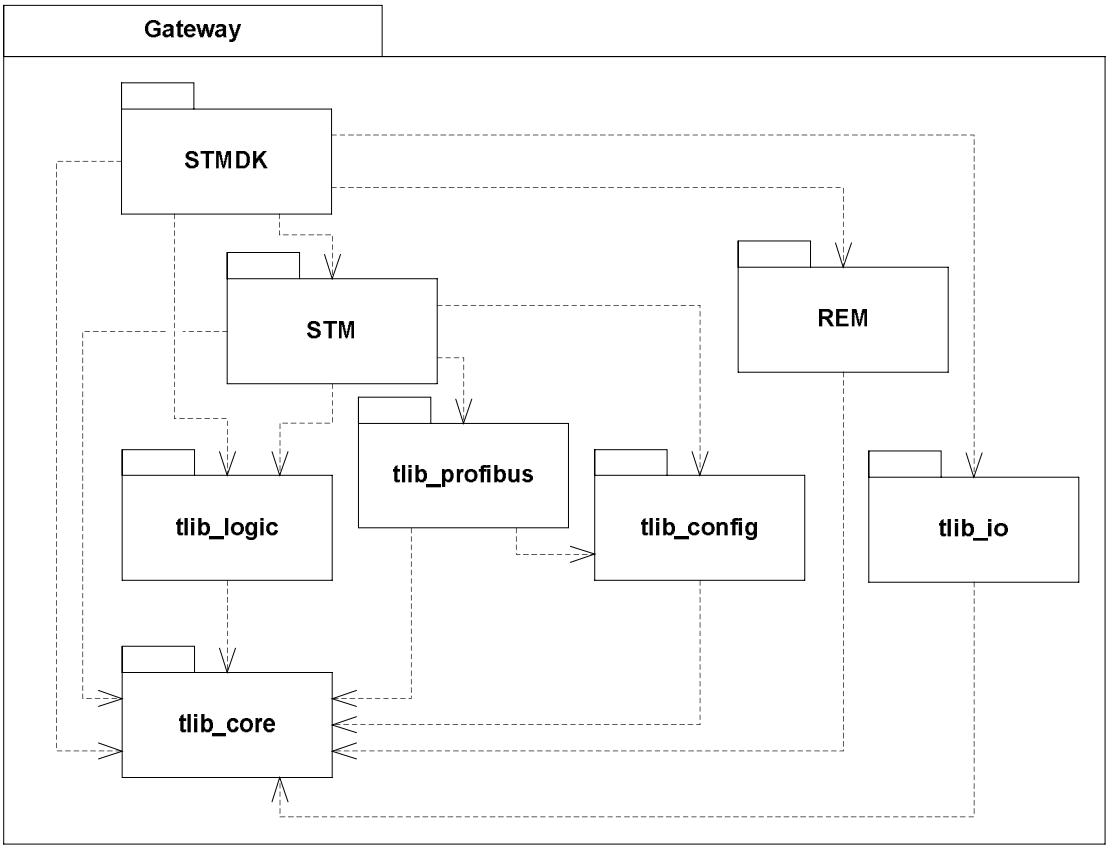
TCC platformens basis software er udviklet og assesset til at opfylde SIL4 kravene givet i [EN50129].

ZUB123 task'ets funktionalitet er ikke ændret i porteringen fra den eksisterende platform til TCC platformen. Funktionaliteten efter porteringen eftervises ved at gennemføre den eksisterende trafikale del af test-suiten, som er udviklet og godkendt til at eftervise den eksisterende ZUB123 software.

Udviklingen af Gateway'en har fulgt Siemens eget procesværktøj, Peacc+. Peacc+ er Siemens måde at realisere Cenelec EN50128.
Peacc+ er udviklet for at øge kvaliteten af det færdige produkt ved at hjælpe projektmedarbejderne gennem de forskellige processer, som er nødvendige, for at opnå et SIL4 produkt. Peacc+ er baseret på forskellige roller, som skal gennemføre forskellige operationer i forskellige processer. Hver proces er beskrevet, så det er klart for de implicerede roller, hvad de hver især skal fortage sig. Peacc+ har været anvendt globalt i Siemens koncernen til flere SIL4 produkter.
Kvaliteten af software-produktet sikres ved at gennemføre processen med udviklingsretningslinier, verifikation, validering og assessment.

Gateway'en er skrevet i programmeringssproget C++ (32 bit) og er opbygget som i Figur 17. Figuren viser afhængigheden af de forskellige software komponenter.

Komponenterne er arkitektonisk opdelt i lag og designet således, at en komponent kun må være afhængig af en komponent på et lavere lag. tlib_core er det nederste lag, hvilket også fremgår af Figur 17.



Figur 17, Package diagram af software komponenten Gateway.

Komponenten STM er den generiske STM, som modsvarer kravene tilhørende [SUBSET-058] og DK-STM dækker funktionalitet til de danske krav.

Komponenterne foruden for DK-STM stammer fra TCC's software biblioteker, som er nærmere beskrevet i afsnit 4.2.1 TCC's software biblioteker

4.2.1 TCC's software biblioteker

4.2.1.1 tlib_core

tlib_core er et basis klasse bibliotek for applikationer kørende på TCC platformen. Biblioteket indeholder blandt andet.

- Sikre data typer (TSafeInt32, TCyclic32, TString o.s.v.)
- TSignalManager (fordeling af events modtaget fra operativ systemet)
- TFile (file handlers)
- TSerialInterface (seriel kommunikation)
- TOStream (data streams)
- TRealTimeClock (sand tids klok)
- TTime (timer events)
- TApplication (fundament for tlib applikation)

TApplication er grundklassen for alle applikationer baseret på tlib.
TApplication::cycleEvent() kaldes periodisk – hyppigheden reguleres ved at ændre

periodetiden. Klassen har indbygget en watchdog, som overvåger, at applikationens task ikke overstiger en fast defineret overvågningstid.

4.2.1.2 tlib_config
tlib_config pakken byder på en konfigurations-parser for filer, der er bygget op omkring Windows-INI syntaksen. De indlæste konfigurationsfiler gemmes i en intern konfiguration database, som nemt og sikkert kan kaldes.

4.2.1.3 tlib_logic
tlib_logic er et framework til håndtering af tilstandsmaskiner. Tilstandsmaskinen beskrives i et dedikeret sprog, som oversættes til byte-kode. Byte-koden fortolkes herefter af TLogic klassen, som er en del af tlib_logic klasse biblioteket.

4.2.1.4 tlib_profibus
tlib_profibus biblioteket indeholder en række klasser, som til sammen danner et PROFIBUS interface på applikationsniveau.

4.2.1.5 tlib_io
tlib_io giver et objekt-orienteret interface til LogIO, der er driveren til bit-vise operationer til periferi-hardware'en.

4.2.1.6 REM
REM står for remanent ram/FRAM - det mister ikke sin information ved strømafbrydelse. Biblioteket gør det muligt at adressere denne hukommelse vha. file handlers. Den tilgængelige hukommelse kan opdeles i flere sektioner, som hver får tildelt sin egen file handler.

4.2.2 Design- og implementeringsmetoder
Gateway komponenten bliver designet ud fra metoderne beskrevet i [EN 50128].

Metoderne B.15, B.20 og B.27 er samlet en godkendt kombination for at opnå sikkerhedsniveauet SWSIL4.

4.2.2.1 Defensiv programmering (B.15)
[CodingStandard] indeholder forskellige regler for defensiv programmering, f.eks. 4.2.1, 5.8.1 og 7.3.3.

4.2.2.2 Fejldetektering og korrektion koder (B.20)
Softwarearkitekturen indeholder en diagnosemekanisme.

4.2.2.3 Fejldetektering og diagnose (B.27)
Konfigurationsdata er beskyttet med MD4 hash kode både under indlæsning og skrivning til remanent hukommelse.

Sikkerhedsrelevant PROFIBUS kommunikation beskyttes ved brug af Safe Time og Safe Link Layers specificeret i [SUBSET-056] og [SUBSET-057]

Seriel kommunikation stammende fra det eksisterende ZUB123 system er beskyttet med check sum.

4.2.2.4 Re-try genetableringsmekanisme (B.53)
Re-try genetableringsmekanisme er brugt på PROFIBUS interface'et. Kommunikationsfejl bliver efterfulgt af en afbrydelse og en genetablering af forbindelsen. Når forbindelsen er genetableret re-transmitteres beskeden.

4.2.2.5 Data indkapsling (B.36)
Alle medlemsvariabler erklæres "private" (regel 8.1.5 [CodingStandard])

4.2.2.6 Variable parameter begrænsning (B.43)
Regel 8.1.5 [CodingStandard] forbyder brug af variable parameter lister.

4.2.2.7 Enkelt returnering fra sub-rutiner og funktioner (B.43)
Regel 7.4.1 [CodingStandard] forbyder funktioner med flere returneringssteder.

4.2.2.8 Kode standarder foreligger (B.16)
Design og implementering følger kodestandard [CodingStandard].

4.2.2.9 Kode stil/formaterings guide (B.16)
Der foreligger projektspecifikke regler i [CppStyleGuide].

4.2.2.10 Ingen Dynamiske objekter (B.16)
Brug af operatorne new og delete er kun tilladt i STM State PO (Power On). Derefter vil brug af disse operatorer medføre nedlukning af systemet.

4.2.2.11 Begrænsninger af pointere (B.16)
Brugen af pointers er reguleret af reglerne 5.5.4, 5.5.5, 5.5.8, 5.7 og 5.9.1.

4.2.2.12 Begrænsninger af rekursion (B.16)
Rekursion er kun tilladt i situationer, hvor afslutningen af rekursionen kan dokumenteres.

4.2.2.13 Ingen ubetingede hop (B.16)
Ubetingede hop er forbudt ifølge regel 7.1.1 and 7.1.2 [CodingStandard].

4.2.2.14 Analyserbare programmer (B.2)
Software arkitektur og design følger regler for struktureret og objekt-orienteret programmering.

4.2.2.15 Strongly Typed programmeringssprog (B.57)
C++ Compiler supportere type-check. Omgåelse af disse type-check (f.eks brug af void pointere eller preprocessor macros) skal ske ifølge [CodingStandard].

4.2.2.16 Struktureret Programmering (B.61)
Strukturerede programmeringsmetoder er brugt i software designet.

4.2.2.17 Programmeringssprog (B.16)
Software komponenten Gateway, skal implementers i C++ med de restriktioner specificeret i [CodingStandard], [CppStyleGuide] og valideringsrapport [GUT-CodingStandard].

4.2.2.18 Valideret oversætter (B.7)
Til udvikling af software komponenten Gateway bruges CAD-UL C++ compiler, version V4250-TS.

4.2.2.19 Oversætter Proven-in-use (B.65)

CAD-UL compiler'en og dets supporterende tools/værktøjer har været brugt i adskillige udviklingsprojekter på SIMIS ECC og TCC platformen – den er derfor betragtet som "proven-in-use".

4.2.2.20 Biblioteker af verificerede moduler og komponenter (B.40)

Der er ikke benyttet pre-verificeret software moduler fra ekstern kildekode til software komponenten Gateway.

4.2.2.21 Grænseværdianalyse (B.4)

Modultest skal indeholde test af grænseværdier for modulets eksterne interfaces. Der skal være en testcase for hver grænseværdi.

4.2.2.22 Reaktionstiming og hukommelsesbegrænsninger (B.52)

Reaktionstimingstest med hovedvægt på bremserelæerne vil blive udført i integrationsfasen.

4.2.2.23 Interface test (B.37)

Modultest tester modulers interfaces samt dets grænseværdier.

4.2.2.24 Data opsamling og analyse (B.13)

Dokumenter, planer og protokoller udviklet under projektforløbet bliver samlet og arkiveret – se [PEACC+].

4.2.2.25 Objektorienteret programmering (B.68)

Software komponenten Gateway bruger objekt-orienteret design supporteret af UML og de egenskaber C++ programmeringssproget stiller til rådighed.

5 Meddelelser fra DK-STM

5.1 Systemmeddelelser fra DK-STM

DK-STM kan vise systemmeddelelser på DMI, som er beskrevet nedenfor.

5.1.1 ”DK-STM: INDGIV TOGDATA eller RANGER”

Denne besked bruges efter endt rangering, hvor brugeren har mulighed for at indgive togdata eller fortsætte med at rangere.

5.1.2 ”DK-STM: Vent. Togdata overføres”

Denne besked vises i forbindelse med overføring af togdata til DK-STM.

5.2 Fejlmeddelelser fra DK-STM

Fejlmeddelelser fra DK-STM er sammensat af præfikset ”FF” efterfulgt af et trecifret heltal. Beskrivelsen af den pågældende fejlkode findes i Brugermanualen SN655.00 Q2960.

Fejlmeddelelsen bliver vist på DMI med følgende format,

ATC: FFxxx Pzzzz

hvor zzzz er positionen af sidst passeret balise.

Fejlmeddelelserne kan ses på forskellige interfaces – disse er nærmere beskrevet sammen med fejllisten i Brugermanualen.

6 Komponentliste

Følgende oplistede fysiske komponenter indgår i DK-STM.

6.1 SIMIS TCC 19" Rack

Komponent nr. S25160-C2001-A1-.*.
Fabrikant: Siemens AG

6.2 SIMIS TCC VE5A, CPU

Komponent nr. S25391-B90-X23-.*.
Fabrikant: Siemens AG

6.3 SIMIS TCC SERIO5

Komponent nr. S25391-B94-A2-.*.
Fabrikant: Siemens AG

6.4 SIMIS TCC PROFI5

Komponent nr. S25391-B98-A2-.*.
Fabrikant: Siemens AG

6.5 SIMIS TCC SRAUS5-24V

Komponent nr. S25391-B92-A2-.*.
Fabrikant: Siemens AG

6.6 SIMIS TCC SRAUS5-110V

Komponent nr. S25391-B92-A24-.*.
Fabrikant: Siemens AG

6.7 SIMIS TCC TASSE5

Komponent nr. S25391-B111-A2-.*.
Fabrikant: Siemens AG

6.8 SIMIS TCC ÜBGEN5

Komponent nr. S25391-B112-A2-.*.
Fabrikant: Siemens AG

6.9 SIMIS TCC SV5, 24V

Komponent nr. S25515-B4003-A3
Fabrikant: Siemens AG

6.10 SIMIS TCC SV5, 110V

Komponent nr. S25515-B4003-A4
Fabrikant: Siemens AG