DK-STM

System Description

banedanmark	Verified		Address Banedanmark Amerika Plads 15 DK-2100 Copenhagen Ø	Planning Siemens A/S Borupvang 3 DK-2750 Ballerup
	Replaces			
	Approved by Banedanmark			

	Version 1 Date and initials	Last version Date and initials	Drawing name **DK-STM** System Description	
Prepared by	19-11-2014 BBE	23-01-2-12 BBE		
Checked by	19-11-2014 STN	23-01-2012 STN		
Approved by	28-11-2014 STN	23-01-2012 STN		
	Language EN	Version **2.00 19.11.2014**	Drawing no. KN 655.00 Q2959	Page/of pages 1 (41)

Change log

Version/date	Page(s) covered	Description	References
01.00 / 23.01.2012	All	First final publication	
02.00/19.11.2014	All	Baseline3.0 update	

Contents:

1 Introduction

This document is the system description for the DK-STM component. DK-STM is the component that enables ETCS-equipped trains to use the ATC infrastructure. Together with ETCS Onboard DK-STM makes up the ETCS system.

1.1 Purpose

The document is written for technical staff who want to get an overview of the functionality of DK-STM.

The purpose of the document is to describe the functions of DK-STM in order to give the reader an understanding of the tasks performed by DK-STM in the overall ETCS system.

The components used, hardware as well as software, are described and it is explained how a level SIL4 product is obtained through various processes and designs.

In addition, the operating states of DK-STM and its reactions to faults are explained.

1.2 Scope

This document will only describe the functionality and characteristics of a DK-STM.

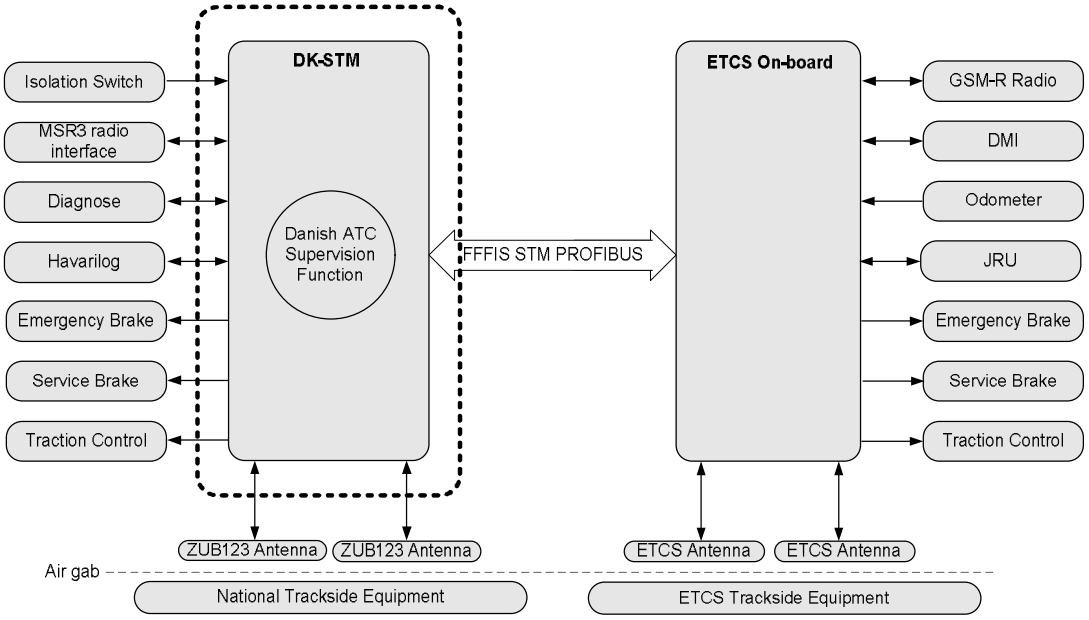

Figure 1: Scope of DK-STM system description

The dotted line in Figure 1 above marks the scope of this document. The ETCS components will not be described in detail in this document, but can be found in [SUBSET-035]. Danish ATC components will be described generally.

As appears from Figure 1 above, DK-STM, like ZUB123, is connected directly to brakes, traction and the serial ATC components. The Isolation Switch is the ETCS name of the isolation switch used to disable (isolate) DK-STM.
Braking and traction commands are simultaneously sent to ETCS through the PROFIBUS connection.

The driver operates DK-STM through DMI. DK-STM only has access to DMI when ETCS has assigned monitoring responsibility to DK-STM.

DK-STM receives odometer data from ETCS.

When DK-STM sends data to the Data Logging Unit, these data are also sent to the ETCS JRU simultaneously.

Definitions

2v2	2 of 2 system – two results are calculated and compared
ATC	Automatic Train Control
CRC	Cyclical Redundancy Checking
DA	Data Available. A state in DK-STM where it is responsible for the train operation
DK-STM	STM dedicated to the Danish infrastructure
DMI	Driver Machine Interface
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FA	Failure. A state in DK-STM where it needs to be restarted to function again. ETCS Onboard is responsible for the train operation
FDL	Field Data Link (PROFIBUS)
FFFIS	Form-Fit Functional Interface Specification
HS	Hot Standby. A state in DK-STM where it is ready to take over responsibility for the train operation. The ATC onboard antennas are active
JRU	Juridical Recording Unit
RBC	Radio Block Centre
RKFS	Processor card release signal
SIL4	Safety Integrity Level 4
SIMIS	Siemens Microprocessor Interlocking System
STM	Specific Transmission Module
TCC	Train Control Computer
TPR	Telegram bit stating the position of the data store (has a value of 0 or 1)

1.3 References

[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 (Protocol for serial communication between ATC, TC, MSR3 and Data Logging Unit, 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 Document Log

00.01	31.03.2011	First version, ready for review	BBE
01.00	01.06.2011	First version	BBE
01.01	30.12.2011	Updated following BDK comments	STN
02.00	19.11.2014	Baseline 3.0 update	BBE

2 General Design

2.1 Conditions and Limitations

DK-STM is a Gateway solution, meaning that the existing functionality from the original Danish ATC master computer ZUB123 can be used again. The Gateway is the link between the ETCS and ATC systems. The source code from the ZUB123 master computer is imported into the new DK-STM platform where it will collaborate with the newly developed Gateway component as two independent programs exchanging information.

2.2 Version 2.3.0.d and Baseline 3.0

In April 2008 the European Railway Agency launched ETCS SRS version 2.3.0d. ETCS SRS Baseline 3.0 will be released in 2012.

When DK-STM has found a compatible ETCS Onboard version, it will be registered in DK-STM and will then be used upon start-up. Afterwards a change of ETCS Onboard version requires operation from a technician.

If no compatible version is found, DK-STM goes to FA state (failure).

2.3 System Description

DK-STM is a component in the overall ETCS Onboard system and the primary task of DK-STM is to monitor a vehicle's movements on the national ATC-equipped lines by means of information from the national infrastructure. The primary functions of DK-STM are:

- To read and decode data from the existing infrastructure via balises and line conductors
- To monitor the correctness of data and trigger an alarm if the data are incorrect or incomplete
- To monitor that the vehicle's movements are consistent with the information from the infrastructure
- To inform the driver about the current operating state via DMI
- To receive interaction from the driver via DMI

Figure 2 is a block diagram of the components included in a Danish/national DK-STM configuration. The blue components are from the existing ATC system, while the green are ETCS components.

Emergency brake, service brake and traction are controlled by both DK-STM and ETCS Onboard (or other STMs for other countries) - these are marked in red. The train does not have two sets of these train components so the systems share one set. ETCS decides unconditionally to which system the use of brakes and traction is allocated.

DK-STM is connected to ETCS Onboard via a PROFIBUS connection. Logically the PROFIBUS connection is subdivided into functions that handle the communication with the peripheral equipment of ETCS Onboard, such as DMI, Odometer, JRU, etc.

The specification of the connection is described at application level in [SUBSET-058].

DK-STM is in charge of the functionality that interfaces with the existing ATC components.
The Isolation Switch, also called the emergency brake suspension switch, is used to isolate the emergency brake (the service brake does not require isolation).
The serial interfaces MSR3 and Data Logging Unit are used in the same way as in the existing ATC system if they are selected in DK-STM's maintenance window – specifications are available in [IN656V1711]. DK-STM does not require a TC (Train Computer) and does consequently not have a TC interface.
Exchange of line information on lines with ZUB123 balises and line conductors (if relevant) takes place in the same way as in the existing ATC system by means of ZUB123 antennas.
The ATC cab signal and the odometer used then have been replaced by a standardised ETCS DMI and an ETCS odometer, respectively, with which DK-STM exchanges data over the PROFIBUS.

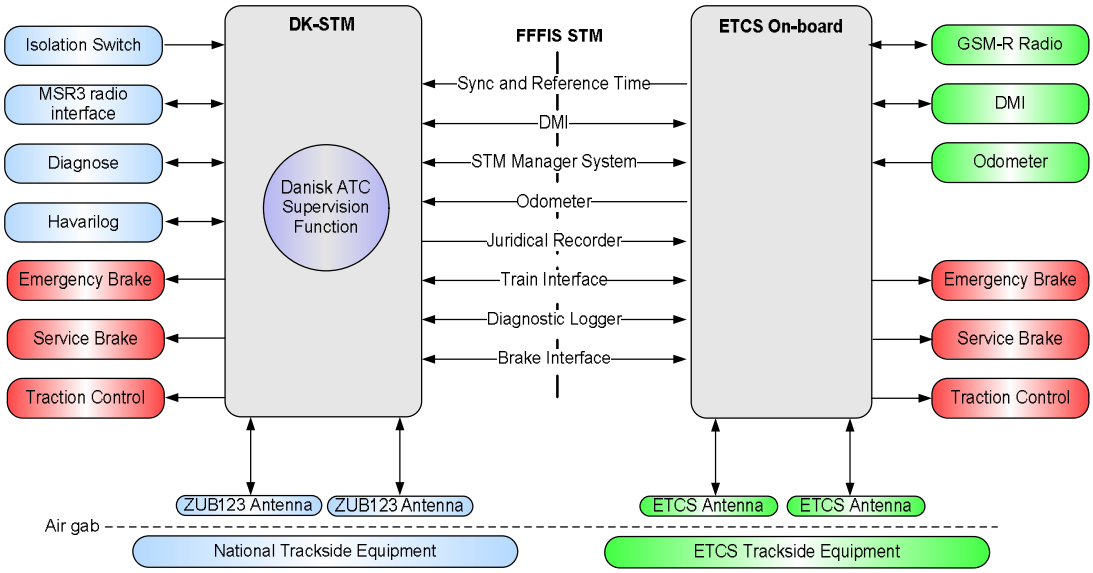

Figure 2: Block Diagram of Components Included in the Danish STM Configuration

2.3.1 The Overall ETCS System with DK-STM

ETCS is specified in various levels – ETCS Levels. The levels reflect the complexity of the systems. Presently, the following levels exist:

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

In ETCS Level 0, ETCS Onboard only monitors that the speed does not exceed the maximum speed entered for the train or the maximum speed stated for the line.

In ETCS Levels 1 to 3, the infrastructure is fully equipped with ETCS line equipment, whereas the original, national equipment is used in ETCS Level STM.

In Denmark ETCS Level 2 has been chosen as the system to replace the Danish ATC System. Figure 3 shows how operation will take place for lines equipped with ATC and lines equipped with ETCS, respectively. As both systems are dependent on a track detection system (axle counters or track isolations), these are not included in the outline.

The ETCS components are marked in green and the blue components are part of the Danish ATC.

Both systems are based on antennas and balises. Via the antennas the balises send line information to the monitoring computer of the train. Many different kinds of line information are sent in the ATC system and based on this information DK-STM can calculate a braking curve. In ETCS Level 2 the balises are simplified; they are only used for determining position and direction of travel. The remaining pieces of line information are transmitted by means of a GSM-R network connecting the trains and the safety systems. In connection with the transition from a traditional signal system to an ETCS Level 2 system, the majority of the optical signals can be left out.

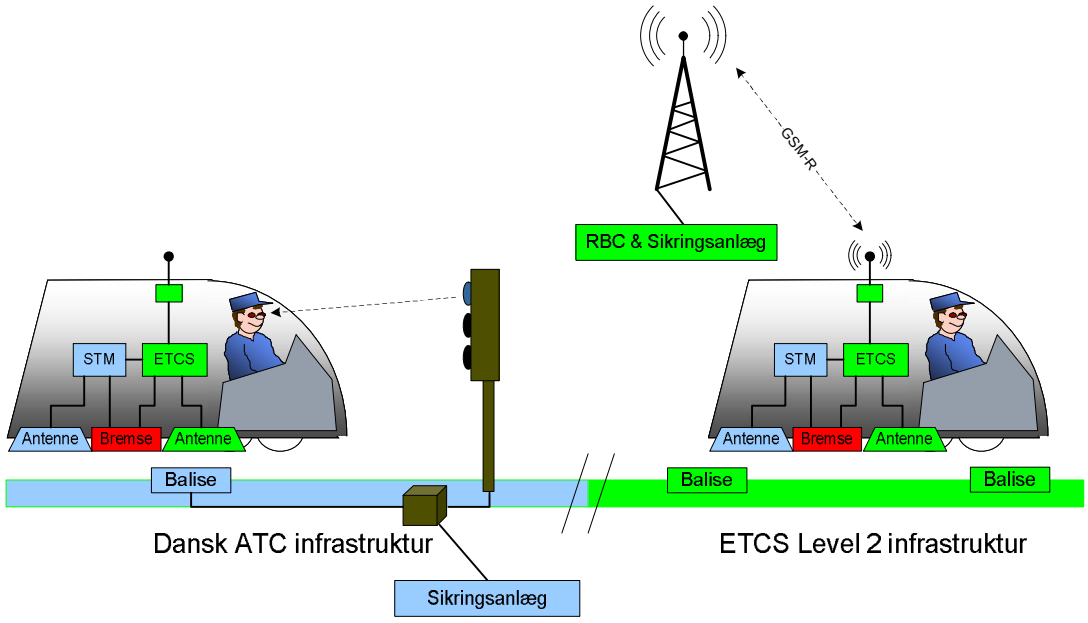

Figure 3: Danish ATC and ETCS Level 2

2.4 DK-STM Hardware

In terms of hardware, DK-STM is built from components from the SIMIS® TCC family. Figure 2.1 shows the schematic structure of a DK-STM in a 19” rack.

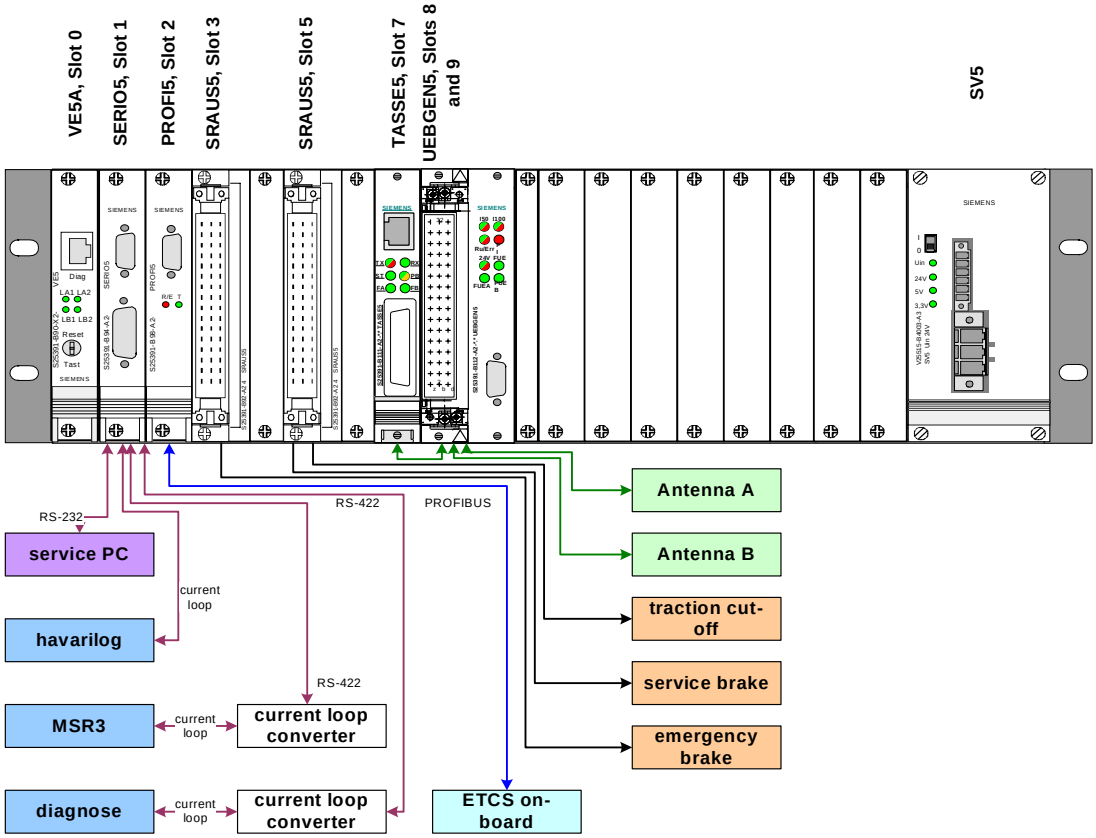

Figure 4: Schematic Structure of a DK-STM

Slot	Component	Use
0	SIMIS TCC VE5, CPU	DK-STM SW Communication with other components
1	SIMIS TCC SERIO5	Communication with Data Logging Unit, MSR3 and Diagnostics
2	SIMIS TCC PROFI5	Communication with ETCS Onboard
3	SIMIS TCC SRAUS5	Communication with emergency brake
5	SIMIS TCC SRAUS5	Communication with service brake and traction cut-off
7	SIMIS TCC TASSE5	Storage of ATC antenna telegrams and control of transmit/receive switch
8	SIMIS TCC ÜBGEN5	Communication with existing ATC antennas
19	SIMIS TCC SV5	Power supply

Table 2.1: Configuration of Basic Frame in DK-STM

The TCC base system is a dual channel computer system (2v2) developed for safety-critical railway applications that are required to fulfil the SIL4 safety level.

2.4.1 SIMIS TCC Basic Frame

The basic frame or the 19” rack is designed to obtain maximum flexibility. In addition to processor cards and power supply the basic frame may be equipped with up to 11 optional peripheral cards plus some dedicated cards for handling of different balise systems.

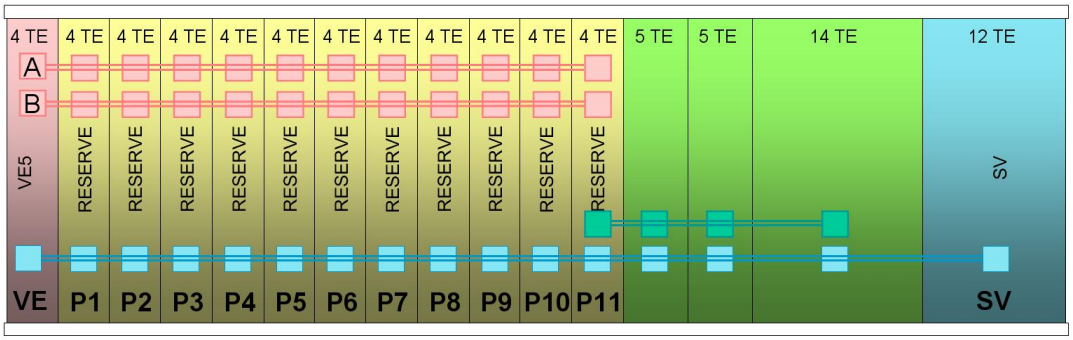

Figure 5: SIMIS TCC Basic Frame

The basic frame has a width of 84 TE (width unit = 5.08mm) and the allocation is as illustrated in Figure 5. Its height is 3 HE (height unit = 44.45mm).

A safe bus (dual channel) connects the CPU card with the 11 peripheral card slots. The busses are used as a safe coupling of the peripheral units and the CPU card.

All card slots receive power from the power supply in the basic frame using the last 12 TE. In addition, a bus is connected between the 11th peripheral card slot and three extra expansion slots that are not connected to the safe bus.

The standard width of a peripheral card is 4 TE. For instance, the SRAUS5 card has a width of 5 TE and consequently takes up two peripheral card slots.

2.4.2 SIMIS TCC VE5, CPU

The VE5 processor card is based on two 80486DX CPUs from AMD, each constituting a CPU channel. They are monitored by a circuit that compares the results of the two CPUs. In case of inconsistencies between the two CPUs, there will be a CPU stop, meaning that all the peripheral cards will return to their safe condition.

The card has 8Mbyte flash ram (FRAM) and 2Mbyte static ram (SRAM).

Programming of the card takes place via a Unilink box that is connected to the card using an RJ45 Ethernet plug and connected to the PC using a USB plug.

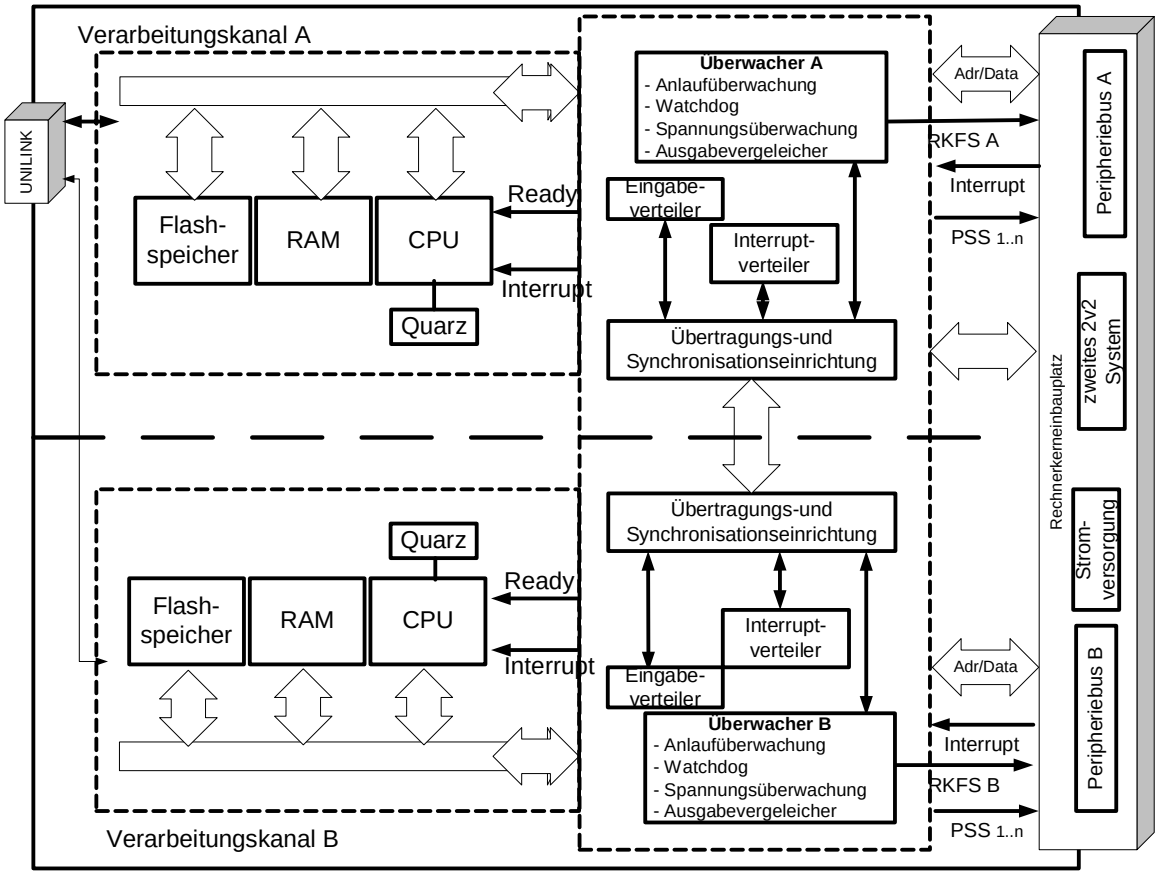

Figure 6: SIMIS TCC VE5 CPU Block Diagram

2.4.3 SIMIS TCC SERIO5

The SERIO5 card is equipped with 5 serial channels. These channels may be configured as RS232, RS422 or as a 20mA current loop.

- 2 RS232/RS422 (up to 19.2kbps)
- 1 RS422/current loop (up to 19.2kbps)
- 1 RS422 (up to 19.2kbps)
- 1 RS232/RS422 (up to 115.2kbps)

In addition, the SERIO5 card also has a built-in RTC (Real Time Clock) with a battery backup and 128kBytes flash ram (FRAM).

2.4.4 SIMIS TCC PROFI5

The PROFI5 card has a PROFIBUS FDL (RS-485) interface, in accordance with the [EN 50170] standard.

2.4.5 SIMIS TCC SRAUS5

SRAUS is an abbreviation of ”safe relay outputs”.

SRAUS is available in 2 versions; a version for 24V and a version for 110V.

The card has relays that are galvanically separated from the peripheral bus by optocouplers. The relays are fed either from the internal 24V supply that is galvanically separated from the external supply or from the external supply that is used to activate the Isolation Switch (protected with a 160mA fuse).

SRAUS5 is fitted with the following:

- 2 safety relay outputs (2 serial make contacts)
- 2 normal relay outputs (single make contact)
- 1 safe overriding input (2 relay coils)
- 3 safety overriding relay outputs (2 serial make contacts)
- 2 normal overriding relay outputs (single make contact)
- 2 normal overriding relay outputs (single break contact)

The relays used are called SR6B4018/SR6B4024 and are from the manufacturer Schrack. The relays are ‘forcibly guided relays‘ according to the EN50205 standard.

Figure 7 shows the two safety relay outputs and the two normal relay outputs. Relays K1, K6, K7 and K8 are controlled via the software. The relay state is read to both channels from two independent measuring points. The black dots each symbolise a pin on the plug mounted on the front of the SRAUS5 card.

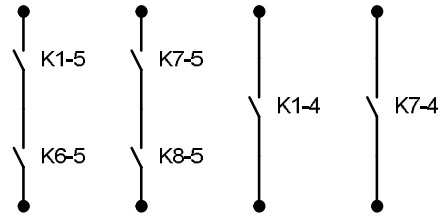

Figure 7: Diagram of Safe/Normal Relay Outputs

Figure 8 shows the two relays and their contact assemblies that make up the safe isolation circuit. Relays K3 and K4 must be activated with 24V/110V.

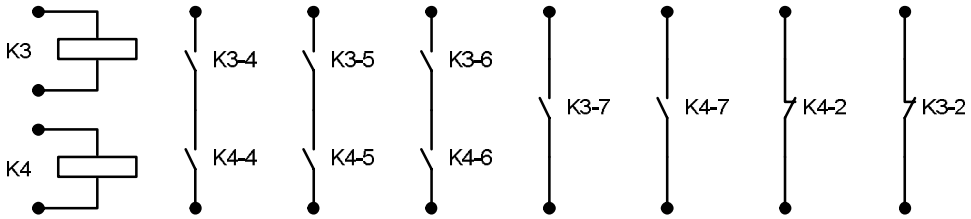

Figure 8: Diagram of Isolation Relays and Their Contact Assemblies

The overriding relays can be used in case of a fault where the emergency brake is activated (one of the braking relays is not on) and you want to haul the train. The overriding outputs must be connected in parallel with the emergency brake relay outputs as shown in Figure 9. In order to carry out an override, relays K3 and K4 must both be activated so as to achieve contact/short-circuiting between”+ Emergency Brake” and”- Emergency Brake”.

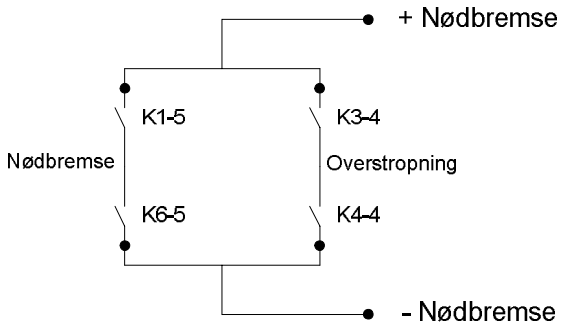

Figure 9: Diagram of Single Emergency Brake Circuit

2.4.6 SIMIS TCC TASSE5

Together with ÜBGEN5, the TASSE5 card forms an integrated interface to the ZUB point antenna.
TASSE is an abbreviation of "**T**elegramm-**A**ufzeichnungs-Baugruppe mit FIFO-**S**peicher und **S**ende/**E**mpfangsumschaltung" and it is used to receive and decode telegrams from the 850kHz data channel.

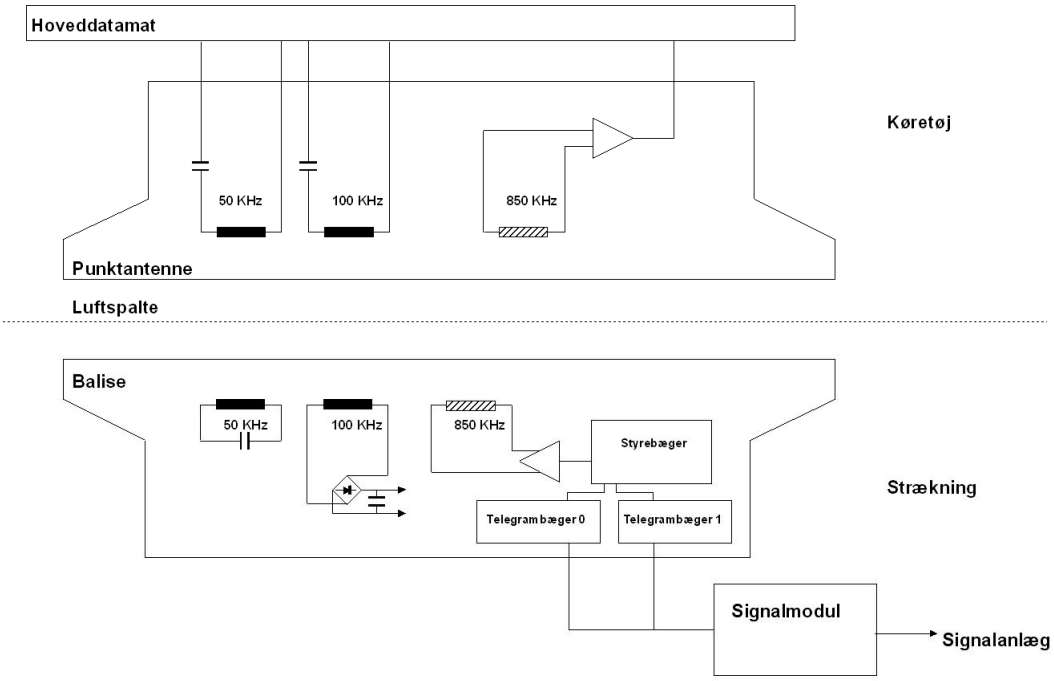

Figure 10: Outline of Point Antenna and Balise

Figure 10 shows an outline of the circuits used for communication over the air gap between the onboard antenna and the balise. The onboard antenna mounted on the vehicle is shown at the top. At the bottom is the balise, controlled by the signal system.

The detection circuit (50 kHz) monitors whether the antenna is placed above a balise.

The energy channel (100 kHz) feeds the balise with inductively transmitted energy.

The data channel (850 kHz) is used to transmit balise data from the telegram data store to the onboard antenna.

The balises receive inductively transmitted energy by means of a series resonance circuit tuned to 100 kHz.

The energy from the 100 kHz is accumulated in a capacitor. When the capacitor achieves a voltage of 18V, the electronics in the balise control data unit are connected.

The access code (2 of 6 code) is read from the signal module or the coded plug. The access code is used to choose a telegram in each of the two telegram data stores.

The maximum 120 bit (96 data bit) long telegrams are transmitted serially to the FM modulator which sends these FM-modulated around the carrier frequency 849kHz (823.5/875kHz), 50kBaud.

Correct balise passage requires detection of the balise and min. three telegrams with identical user data (telegram data exclusive of TPR and CRC bits).

2.4.7 SIMIS TCC ÜBGEN5

ÜBGEN is the abbreviation of ”monitored generator”. The purpose of this card is to detect balises and transmit energy to them.

The balise detection circuit is exclusively used for monitoring whether the antenna passes over a balise. The balise detection circuit is a passive resonant circuit tuned to 50 kHz. The self-inductance of the resonant circuit is wound on a rod of ferrite, which is the antenna. When the onboard point antenna passes over the balise, there will be a power reduction in the 50kHz circuit of the point antenna because the frequency changes in the resonant circuit.

2.4.8 SIMIS TCC SV5

SV5 is the TCC system’s power supply card. The card is available in two versions. A 24V card and a 110V card. In terms of function the cards are identical; the only difference is the input voltage.

- 24V/110V, max. current 4.2A
- 5V, max. current 1.0A
- 3.3V, max. current 4.6A

Card	Power consumption, typical
VE5	2.7W
SERIO5	3.5W
PROFI5	2.3W
SRAUS5	13W (6.5W * 2)
TASSE5	21.7W
ÜBGEN5	5.6W

SV5	10.0W (degree of efficiency approx. 83%, 48.8W)
Total	58.8W

The SV5 card must be fed by a 24V/110V supply with a ripple voltage of less than 2%.

In case of an overvoltage condition (input voltage in excess of 35V/159.5V), a fuse will burn out.

In case of an undervoltage condition (input voltage less than 14V/41.9V), the SV5 software will disconnect.

2.5 DK-STM Software

The DK-STM software mainly consists of two components; the imported component from the ATC master computer which handles the traffic process and a Gateway component which generally enables a conversion between the ETCS and ATC systems.

Figure 11 shows the logical structure of DK-STM. The connections to the surroundings are shown at the perimeter of the diagram. They are connected to some drivers that are used for communication with the hardware. The software parts are linked with lines and arrows in the figure, indicating which way data is transmitted.

The two software components, Gateway and ZUB123, are implemented as two separate tasks carried out in the real time operating system CPM32.

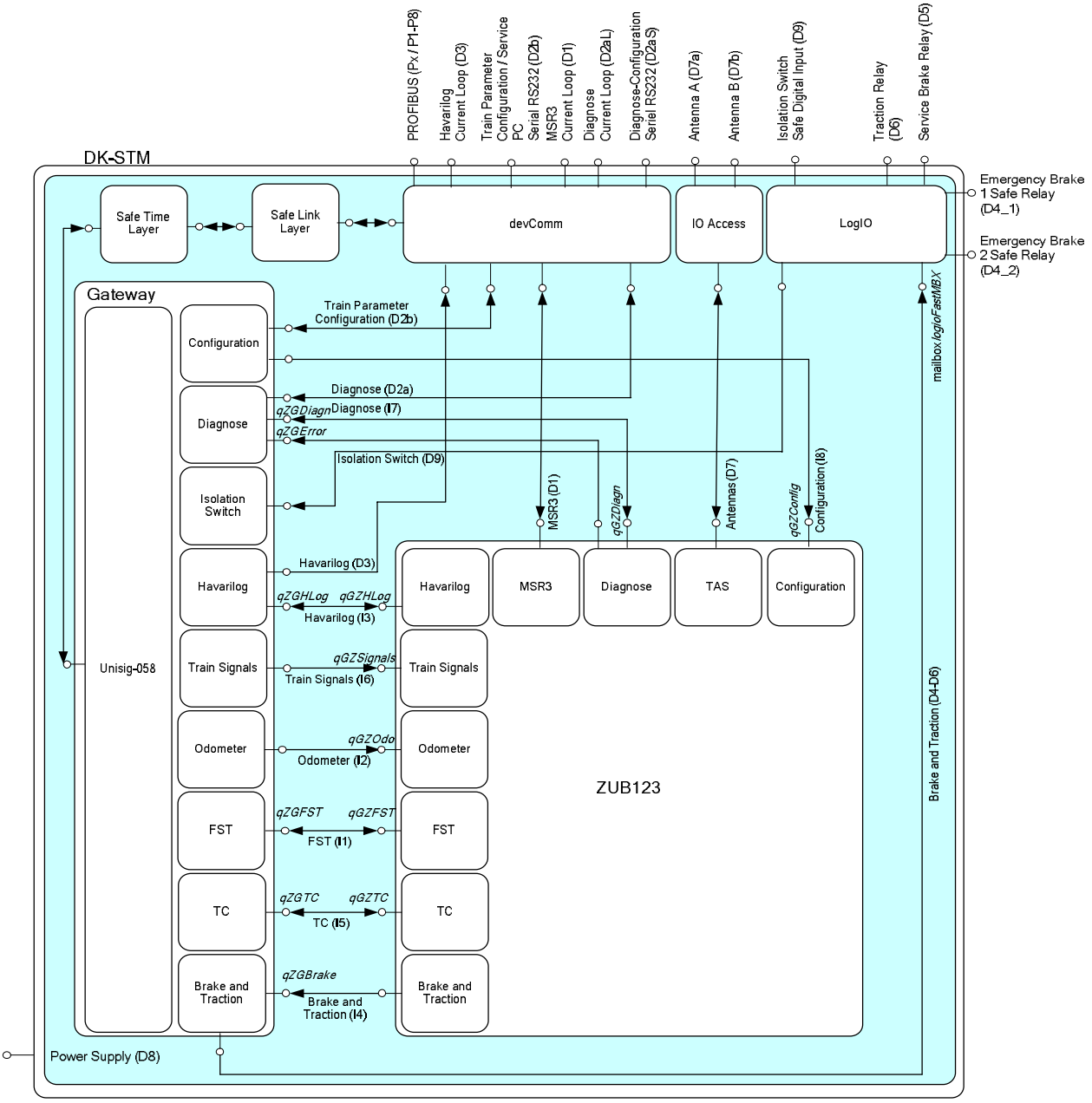

Figure 11: General Software Diagram

2.5.1 ZUB123, the Traffic Process

The traffic process is the software in the existing ATC master computer. The function-related part of the component has not been changed; only the interfaces have been changed. This way it has been ensured that the traffic process remains intact.

The component is programmed in Pascal and works in a separate task. Communication with the Gateway component takes place via queues (data channel). All other communication is through drivers.

The traffic process has the following functions:

- Evaluate and act based on balise information received

- Calculate the braking curve for every 200ms
- Calculate and monitor the current speed
- Transmit ZUB123 diagnostic data
- Transmit ZUB123 Data Logging Unit data
- Exchange data over the MSR3 Radio
- Transmit braking/traction information to the Gateway component
- Transmit ZUB123 state information to the Gateway component via FST
- Receive commands from the Gateway component via FST

The traffic functions are controlled via the connected DMI of the ETCS, e.g. “shunting” and “passage stop”. Indications from the traffic functions are also shown on DMI, e.g. Release ATC “Løs ATC” and Emergency Brake “Nød Bremse”.

2.5.2 Gateway

The Gateway component is the new SIL4 developed component whose purpose it is to be the link between ETCS Onboard and the traffic process.

The Gateway component consists of a generic part which, briefly explained, handles the exchange of STM packets to ETCS Onboard – these are specified in [SUBSET-058]. In addition, the generic part is also the logical state machine described in 3.3. Operating states for DK-STM.

It has been chosen to separate the generic part and the national part in the Gateway component to obtain a design in which the requirements for ETCS and BaneDanmark, respectively, can be completely separate. The national part whose task it mainly is to handle the communication with the ZUB123 component is sent to the generic functionalities.

The Gateway functions in connection with the ZUB123 task are the following:

- Configure ZUB123 and start ZUB123 task
- Set DK-STM in FA if the Isolation Switch is activated
- Convert ETCS Onboard odometer data to odometer pulses (corresponding to the impulse giver previously used)
- Send cab data to ZUB123 by means of Train Signals
- Transmit train data to ZUB123 by means of TC interface
- Read position from the balise last passed by means of TC interface
- Control the ZUB123 monitoring condition by means of FST interface
- Read ZUB123 information by means of FST interface
- Read the ZUB123 braking status and activate the brake if required
- Retransmit diagnostics and data logging unit data

The Gateway functions in connection with ETCS Onboard are the following:

- Exchange DMI information – control of user interface
- Receive odometer data
- Transmit diagnostics and data logging unit data
- Transmit status on emergency brake, service brake, and traction commands

2.5.3 Drivers

The drivers are the software that enables communication with peripheral equipment.

2.5.3.1 DevComm

DevComm is the driver used for peripheral cards with serial communication.

2.5.3.2 IOAccess

IOAccess is an interface which i.a. offers:

- Port-oriented access to the hardware
- Signal in case of change of state
- Processing of interrupt

2.5.3.3 LogIO

LogIO is a task used in connection with bitwise reading/writing operations with peripheral equipment. It automatically updates the user of a particular bit on a peripheral card if its state changes. This is i.a. used with the SRAUS5 card when you wish to set/read the state of individual relays.

2.5.3.4 Safe Link Layer & Safe Time Layer

The PROFI5 card works at PROFIBUS FDL level. In order for the Gateway software to be able to communicate with ETCS at application level, two intermediate layers are required. They are called Safe Time Layer and Safe Link Layer. They are specified in [SUBSET-056] and [SUBSET-057], respectively.

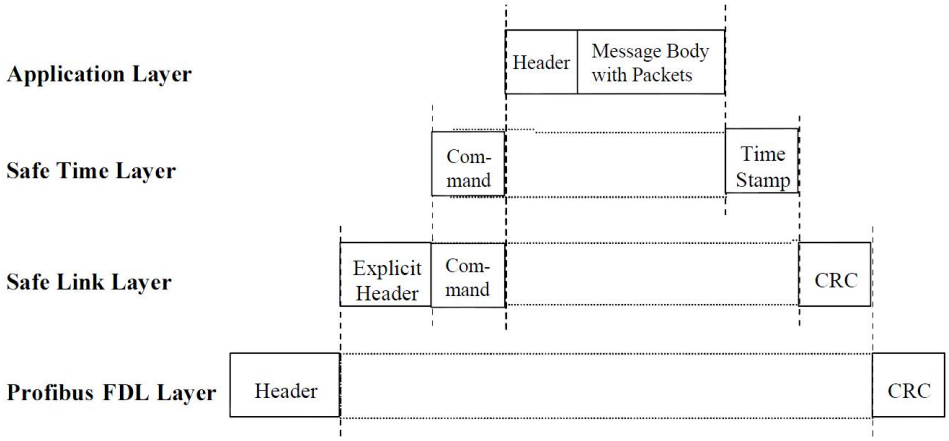

Figure 12: PROFIBUS, STM FFFIS Layers

3 Main Functions of DK-STM

3.1 The Role of DK-STM in the Overall ETCS System

DK-STM is to be used in the transitional phase while the ETCS infrastructure is being implemented. In this transitional phase the lines will have different train control systems. Some lines will be equipped with the Danish ATC, while others will be equipped with ETCS.

On the lines where the Danish ATC has not yet been replaced with ETCS equipment, DK-STM forms part of the ETCS Onboard part to monitor the Danish ATC operation and communicate with the ETCS Onboard system.

The old and well-known ATC cab signal will be replaced by the new ETCS driver machine interface (DMI). Consequently, ETCS and DK-STM can be operated by means of the same operating unit.

3.2 Operation with ETCS

3.2.1 Operation with ETCS on Lines Equipped with ETCS

The line has Euro Balises which function as distance marks – their sole purpose is to state a position and determine in which direction the train is moving.

The outer signals are not used. Movement authority (MA) is transmitted via Euro Radio/GSM-R from RBC (Radio Block Centre) to ETCS Onboard.

ETCS Onboard has sole responsibility for the monitoring and braking in case of danger. Braking curves will be calculated on an ongoing basis based on information received from the Euro Balises and the Euro Radio.

DK-STM is in hibernation mode, meaning that the ATC onboard antennas are not active and that any Danish ATC Balises are ignored.

3.2.2 Operation with ETCS on Lines not Equipped with ETCS (DK-STM)

ETCS Onboard has passed on the monitoring and braking responsibility to DK-STM.

DK-STM uses the existing ATC line equipment for calculation of braking curves, if required. With DK-STM responsible for monitoring it is possible to use all operating patterns available in the Danish ATC - these are listed below.

ATC operating patterns:

- Operation under normal conditions on lines with stationary ATC systems
  - Operation with ATC monitoring
  - Leaving a station
  - Presignalling
  - Approaching a station
  - Speed reductions
  - Stop and move forward to the next signal
  - Automatically protected level crossings

- Operation under normal conditions on lines with stationary ATC train stopping systems
    - Operation with ATC train stopping
    - Leaving a station
    - Presignalling
    - Approaching a station
    - Speed reductions
    - Stop and move forward to the next signal
    - Automatically protected level crossings
- Operation under normal conditions on lines without stationary train control systems
- Shunting
- Operation with ATC during irregularities
    - Shunting into/out of the station and authority to pass a signal
    - Written authority to leave a station and pass a signal
    - Disconnection of ATC system
    - Message
    - Fault

In this operating state both the ETCS and ATC antennas are active. The ETCS antenna is active because it must be possible for ETCS Onboard to switch to another infrastructure if the train leaves the area with ATC line equipment (passing of two ETCS border balises).

3.2.3 Transition between Lines Equipped with ETCS and Lines not Equipped with ETCS

In the areas with transition between ETCS and ATC the transition line will be equipped with both systems.

The normal procedure will be:

The train will first meet an advanced ETCS Balise group indicating the distance to the transition. ETCS Onboard places DK-STM in ”Hot Standby”, which allows DK-STM to activate the ATC antennas.

Later the train will pass an ATC Balise with national line information, enabling DK-STM to calculate a braking curve. The monitoring responsibility still lies with ETCS Onboard.

The border is marked with an ETCS border balise group. When this group is passed, ETCS Onboard orders DK-STM into the “Data Available” state, meaning that DK-STM has the monitoring responsibility.

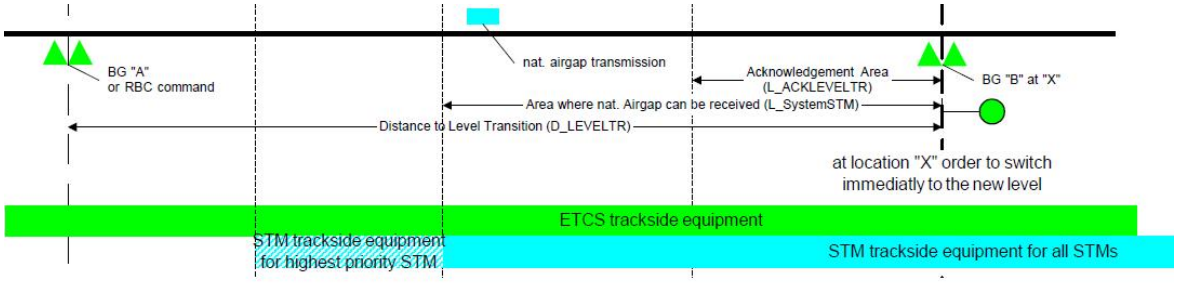

Figure 13: Example of Transition Area

3.2.4 Transition between Two Lines that Are Not Equipped With ETCS

The transition between two STMs is very similar to the transition from ETCS to STM. However, the transition area will be equipped with line equipment for both countries as well as ETCS equipment.

ETCS Onboard still has command and will assign monitoring responsibility from one STM to the other STM when the ETCS border balise group is passed.

3.3 Operating States for DK-STM

DK-STM follows the operating states that are also called STM States in ETCS terminology. STM States are described in [SUBSET-035], chapter 7.3.

Below is a brief description of the individual states.

3.3.1 No Power (NP)

No supply voltage is connected to DK-STM.

3.3.2 Power On (PO)

When supply voltage is connected to DK-STM, its state changes to PO. In the PO state, a self test and synchronisation are carried out of the PROFIBUS Safe Time Layer. When this is done, DK-STM establishes the necessary Profibus connections. When these connections are established, DK-STM will request permission to go to CO.

3.3.3 Configuration (CO)

In the CO state, DK-STM is mainly configured with ETCS train data from ETCS Onboard. After the data exchange DK-STM will request permission to go to DE.

The following parameters are exchanged in DK-STM:

- Length of train
- Max. speed

3.3.4 Data Entry (DE)

The DE state is used to configure DK-STM with the four specific types of train data. The following parameters are exchanged in DK-STM:

- Length of train (value from ETCS train data is used. Can only be changed in connection with entry of ETCS train data)
- Brake percentage
- Max. speed (value from ETCS train data is used. Can be changed in DE)
- ATC direction

The values are entered by means of ETCS DMI.

The DE state is only used this once in connection with the start-up procedure.

If DK-STM needs new, specific train data during STM operation, e.g. after shunting, these data may be requested without going via the DE state by entering new ETCS train data. Then DK-STM will request the four specific types of train data again.

When DK-STM has received its specific train data, it will request to go to CS.

3.3.5 Cold Standby (CS)

In the CS state, DK-STM is initiated, tested and fully configured. DK-STM is not authorised to have activated antennas in the CS state and can consequently not receive line information from the track.

3.3.6 Hot Standby (HS)

In the HS state, the antennas are activated and DK-STM can now receive information from the balises in the track.

DK-STM is ready to take over the monitoring responsibility – it needs only a command from ETCS Onboard.

3.3.7 Data Available (DA)

DK-STM has taken over the monitoring responsibility and operation is according to the Danish ATC rules, i.e. it is possible to use the old cab signal functions via ETCS DMI.

Only in the DA state does DK-STM have the right to use the brake; in all other states ETCS Onboard handles the braking function. DK-STM has a direct connection to the brake. At the same time DK-STM gives braking/traction commands to ETCS Onboard.

3.3.8 Failure (FA)

There has been an unexpected action in DK-STM. When DK-STM is in FA, ETCS Onboard takes over the monitoring function and the emergency braking (if relevant).

The FA state is a “final” state, i.e. DK-STM needs to be turned off and started again from the NP state.

3.4 Operating Incidents for DK-STM

The first four STM states (**NP**, **PO**, **CO** and **DE**) could be called preparation or rigging states. When DK-STM has been rigged and is in the STM state **CS**, these

four states can no longer be accessed until DK-STM has been disconnected from the power supply.

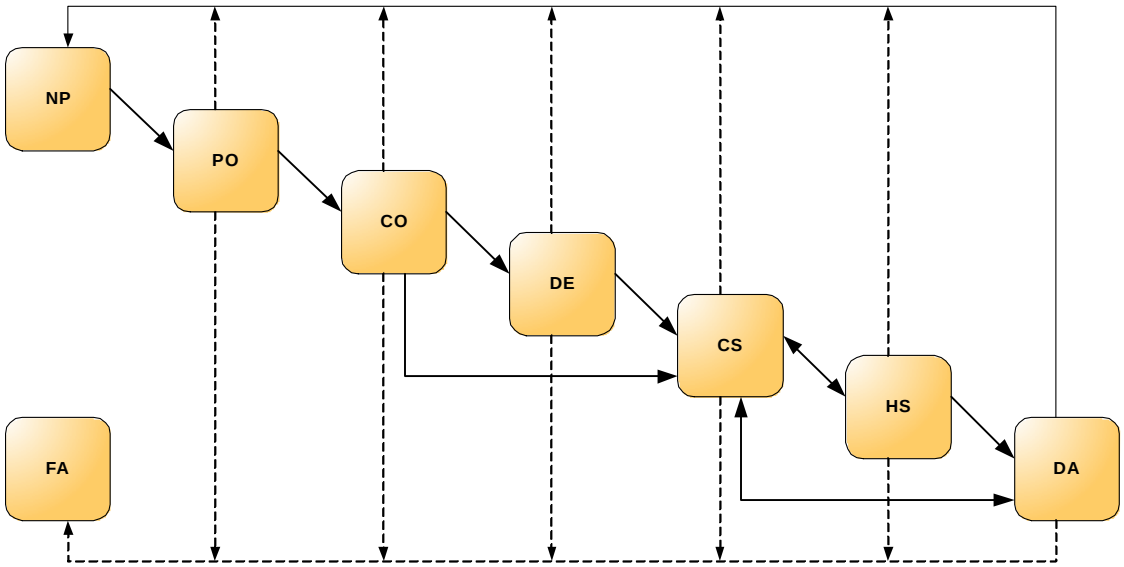

Figure 14: Possible STM State Transitions

The three most interesting states are **CS**, **HS** and **DA**, which can be described as *hibernation*, *ready for monitoring* and *monitoring active*, respectively.

ETCS Onboard alone decides the operating state of DK-STM. DK-STM is only authorised to go to **FA** in case of an unexpected action or the virtual state **NP** if there is no power.

3.4.1 TRIP Operation

In case of emergency braking through a transition from ZUB123 to ETCS, ETCS will go to TRIP operation and continue applying the emergency brake until the train has been brought to a standstill.

Particularly, en emergency braking procedure will be begun if DK-STM is being shunted and passes a transition.

4 Safety

This chapter explains the design considerations made to ensure a hardware/software solution that fulfils the SIL4 requirements.

4.1 Hardware

DK-STM is based on Siemens' SIMIS® TCC Hardware platform which has been designed for safety-critical railway applications according to the specifications stipulated in [EN 50129] for a SIL4 system.

The hardware is an "off-the-shelf item" from Siemens and it is used in a number of railway applications today – consequently the theoretical safety of the TCC hardware is described as proven-in-use.

The system is designed according to the dual channel principle, 2v2. The processor card VE5 has two processors which are synchronised. They run identical codes which are compared by a monitoring module. The monitoring module continuously makes sure that no action is performed due to hardware faults from either of the two processor channels. Figure 6 shows a diagram of VE5.

The VE5 card is also connected to the peripheral cards by means of the 2v2 principle. Both processing channels are led to the peripheral cards (Channel A and Channel B), each by means of a parallel-connected bus consisting of the following connections.

8 bit	Address/data bus
1 bit	Clock
16 bit	Peripheral card selector
1 bit	Release signal (RKFS)
1 bit	Common interrupt

Table 1: Bus Signals for One Channel

The monitoring module includes a watchdog which ensures that a task does not exceed its pre-defined execution time, e.g. if the CPU cannot handle the load.

The voltage supply, SV5, is also monitored by VE5. In case of a poor or failing supply this will also lead to a safe reaction.

4.1.1 Emergency Brake

The emergency brake circuit is designed according to the principle that if there is a relay fault in the SRAUS5 card, it will lead to a disconnection of the switches connected to the brakes so that they become inactive and brake the train. Relay faults are detected by a program that tests the state of the relays. In case of a power failure the switches will also disconnect and brake the train. Even if a relay is welded the design with the serial connection of two independent relays will provide a safe disconnection of the brakes.

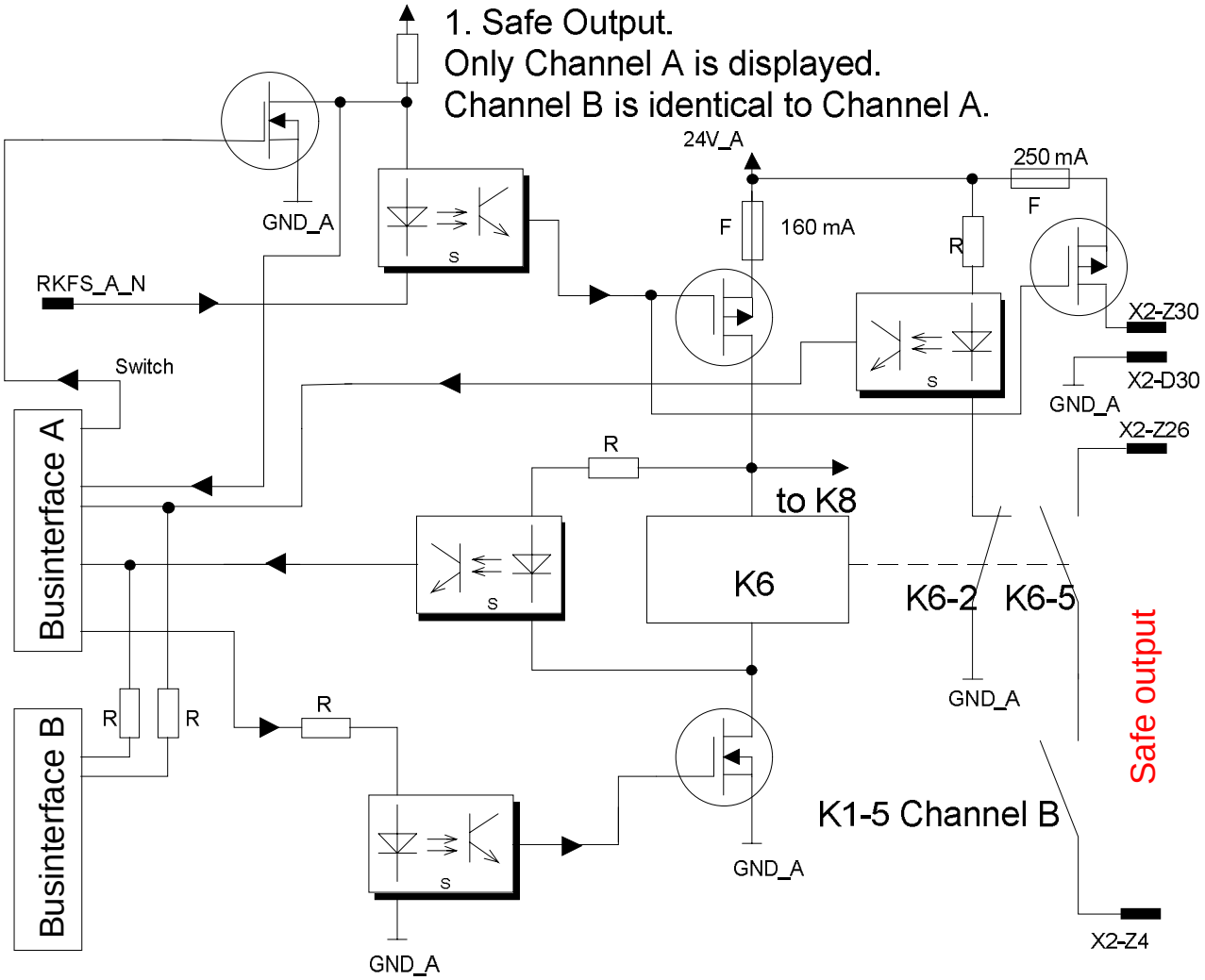

Figure 15: Diagram of One Channel of a Safe Relay Output

4.1.1.1 Dual Channel System

Figure 15 is a diagram of the components that make up one of the two channels of the safe brake circuit. The safe output it controlled by relays K6 (Channel A) and K1 (Channel B – not illustrated).

There are three conditions that must be met for relay K6 to come on:

- The card must be released by the process card VE5 by means of the RKFS signal
- The switch from bus interface A must be activated
- The signal from bus interface A which controls the bottom MOSFET must be activated

The state of relay K6 is measured at two independent measuring points. Measurements are made of the voltage potential across the relay coil and the state of brake contact assembly K6-2.

The design between the two independent channels is in compliance with the specifications in [EN 50129], D.2.1, regarding primary independence.

Secondary independence according to [EN 50129], D.2.2, is obtained by means of the two independent RKFS signals from the processor card.

4.1.1.2 Cyclic Test

Cyclic tests of the relays included in the two safe outputs (K1, K6, K7 and K8) will reveal any defects (contact assemblies in unexpected position) within one second. A defect will lead to a safety cut-out.

Faults on the bus interface up to and including control of relay coils will be detected through cyclic tests within half an hour and lead to a safety cut-out.

4.1.1.3 Galvanic Separation

Galvanic separation is obtained through the use of optocouplers. They have been tested by means of test voltage pulses of 1500V (distance 2.5mm).

4.1.1.4 Overcurrent Protection

The relay coils are protected with fuses of 160mA – typical current is 90mA.

4.1.2 Service Brake

The service brake does not have a safe output as it is not safety-critical.

4.1.3 Isolation Switch

The isolation circuit for Channel A is shown in Figure 16. The design of Channel B is identical.

Relay coil K4 needs an outside voltage of 24V to activate the isolation of Channel A. This must also be done for Channel B (K3) to short-circuit the two series-connected make contacts (K4-5 and K3-5).

The relay state is read to both bus interfaces for both channels.

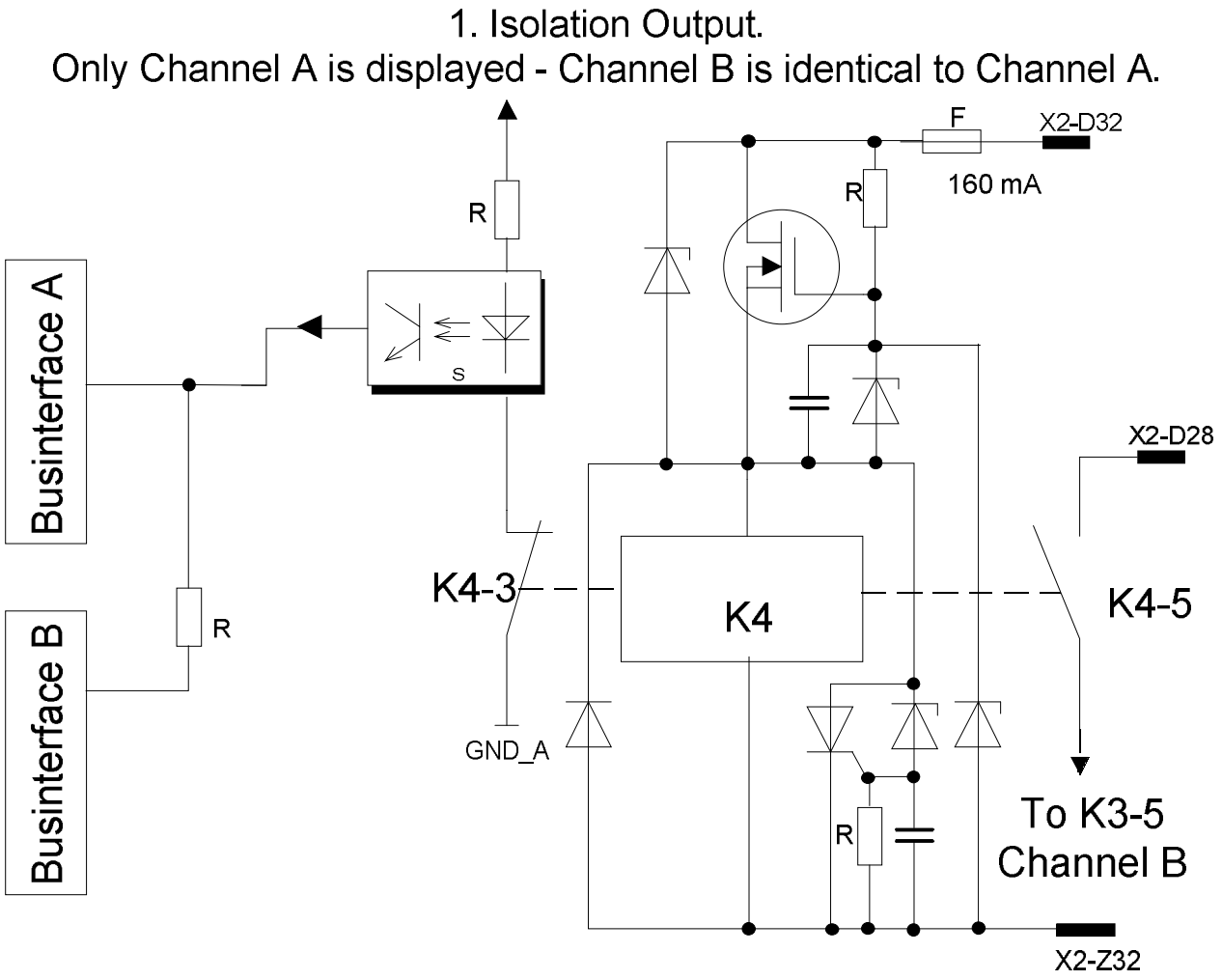

Figure 16: Diagram of One of the Two Isolation Channels

4.1.4 Traction

The traction does not have a safe output as it is not safety-critical.

4.1.5 Serial Communication

In terms of software, serial communication is secured by means of a check sum. In addition, the PROBIBUS is protected by Safe Link and Safe Time layers.

4.1.6 ZUB123 Antennas – Air Gap

The existing ATC system includes many measures to ensure that the communication over the air gap takes places in a safe and reliable manner.

The balises are equipped with two telegram data stores, each with its own TPR bit. TPR states the position of the telegram data stores – which can be either 0 or 1.

Balise data are received in a serial dual channel system. The balise alternatively sends telegrams from the two telegram data stores. User data from the two telegram data stores must be identical - they are compared upon receipt.

Which telegram that is sent from a telegram data store is chosen by means of a 2 of 6 code. The two telegram data stores are controlled by two independent 2 of 6 codes.

Correct balise passage requires detection of the balise and min. three telegrams with identical user data (telegram data exclusive of TPR and CRC bits).

The balises are coupled with a distance parameter indicating when the train is expected to receive new balise data. Information about whether this safety measure is active is included in the telegram data. It is possible to deactivate this safety measure.

Balise data are protected by an 8 bit long CRC.

Antennas may only be adjusted by authorised staff. The adjustment is made via a sub-menu in DMI which is protected by a password.

4.2 Software

The software in DK-STM consists of three main blocks:

- TCC basic software
- The ZUB123 task, the traffic process from the ATC master computer
- The Gateway task

The basic software of the TCC platform is developed and assessed to comply with the SIL4 requirements stipulated in [EN50129].

The functionality of the ZUB123 task is not changed when ported from the existing platform to the TCC platform. The functionality after porting is checked by carrying out the existing traffic part of the test suite developed and approved for checking the existing ZUB123 software.

The development of the Gateway followed Siemens' own process tool, Peacc+. Peacc+ is Siemens' implementation of Cenelec EN50128.
Peacc+ has been developed to increase the quality of the finished product by helping the project employees through the various processes that are necessary for creating a SIL4 product. Peacc+ is based on various roles that must complete various operations in various processes. Each process is described in such a way that it is clear to the roles involved what they are each supposed to do. Peacc+ has been used globally in the Siemens Group for several SIL4 products.
The quality of the software product is ensured through the completion of the process with development guidelines, verification, validation and assessment.

The gateway is written in the programming language C++ (32 bit) and is structured as shown in Figure 17.
The figure shows the dependence on the various software components.

«In terms of architecture the components are divided into layers and designed in such a way that a component can only be dependent on another component in a lower layer. As appears from Figure 17, tlib_core is the bottom layer.

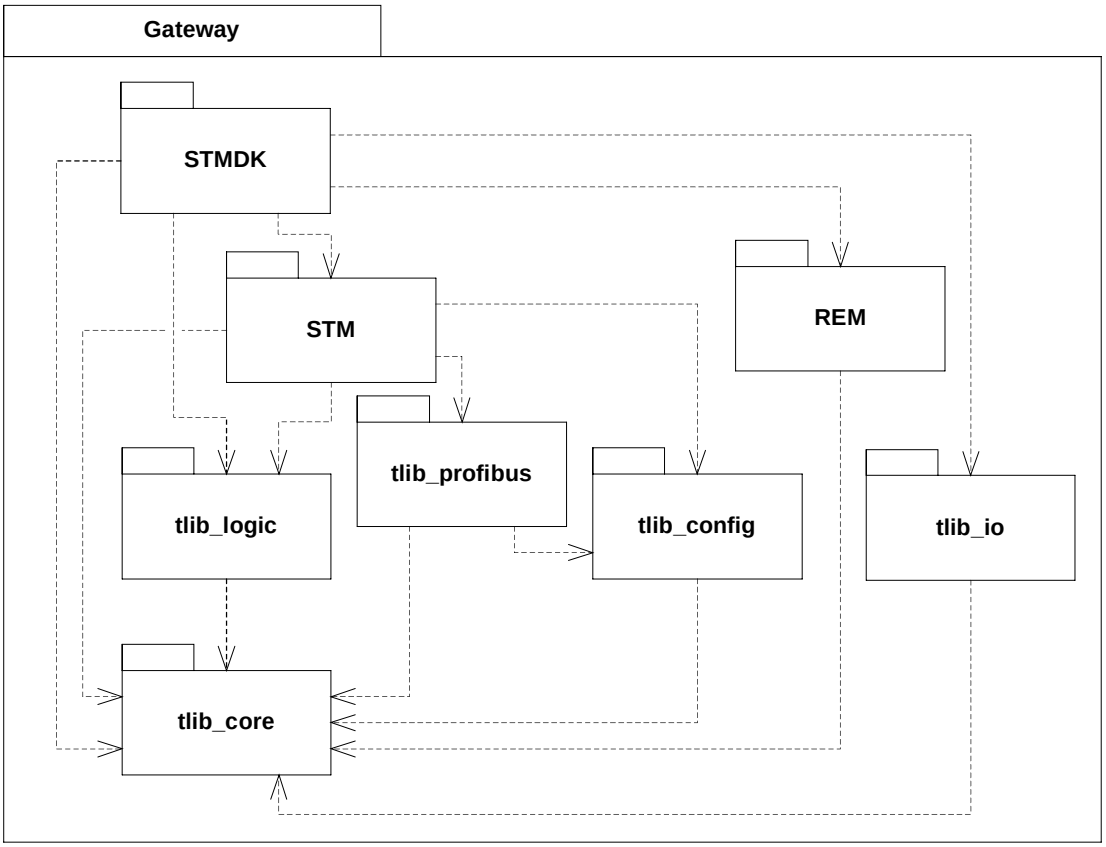

Figure 17: Packet diagram of the software component Gateway

The STM component is the generic STM which fulfils the requirements in [SUBSET-058] and DK-STM covers the functionality according to the Danish requirements.

The components outside DK-STM originate from TCC's software directories which are described in detail in section 4.2.1 TCC's software directories.

4.2.1 TCC's Software Directories

4.2.1.1 tlib_core

tlib_core is a basic class directory for applications that run on the TCC platform. Among other things, the directory includes:

- Safe data types (TSafeInt32, TCyclic32, TString, etc.)
- TSignalManager (distribution of events received from the operating system)
- TFile (file handlers)
- TSerialInterface (serial communication)
- TOStream (data streams)
- TRealTimeClock (real-time block)
- TTime (timer events)
- TApplication (foundation for the tlib application)

TApplication is the base class for all applications based on tlib.
TApplication::cycleEvent() is called cyclic – the frequency is adjusted by changing

the cyclic time. The class has a built-in watchdog which monitors that the application task does not exceed a fixed, defined monitoring period.

4.2.1.2 tlib_config

The tlib_config packet includes configuration parsers for files structured around the Windows-INI syntax. The loaded configuration files are saved in an internal configuration database which can be called easily and securely.

4.2.1.3 tlib_logic

tlib_logic is a framework for handling state machines. The state machine is described in a dedicated language that is translated into byte code. The byte code is then interpreted by the TLogic class which is part of the tlib_logic class directory.

4.2.1.4 tlib_profibus

The tlib_profibus directory has a number of classes which together make up a PROFIBUS interface at application level.

4.2.1.5 tlib_io

tlib_io provides an object-oriented interface to LogIO which is the driver for bitwise operations for the peripheral hardware.

4.2.1.6 REM

REM is an abbreviation of remanent ram/FRAM – it does not lose its information when the power is cut off. The directory enables addressing this memory by means of file handlers. The available memory can be divided into several sections, to each of which a separate file handler is allocated.

4.2.2 Design and Implementation Methods

The Gateway component is designed based on the methods described in [EN 50128].

Methods B.15, B.20 and B.27 together constitute an approved combination to obtain the SWSIL4 safety level.

4.2.2.1 Defensive Programming (B.15)

[CodingStandard] includes various rules for defensive programming, e.g. 4.2.1, 5.8.1 and 7.3.3.

4.2.2.2 Fault Detection and Correction Codes (B.20)

The software architecture includes a diagnostic mechanism.

4.2.2.3 Fault Detection and Diagnosis (B.27)

Configuration data are protected with a MD4 hash code, both during reading and writing to the remanent memory.

Safety-relevant PROFIBUS communication is protected by means of Safe Time and Safe Link Layers specified in [SUBSET-056] and [SUBSET-057].

Serial communication originating from the existing ZUB123 system is protected by a check sum.

4.2.2.4 Retry Restoring Mechanism (B.53)
A retry restoring mechanism is used on the PROFIBUS interface. Communication errors are followed by a disconnection and restoration of connection. When connection has been restored the message will be retransmitted.

4.2.2.5 Data Encapsulation (B.36)
All member variables are declared private (rule 8.1.5 [CodingStandard]).

4.2.2.6 Variable Parameter Restriction (B.43)
Rule 8.1.5 [CodingStandard] prohibits use of variable parameter lists.

4.2.2.7 Simple Return from Subroutines and Functions (B.43)
Rule 7.4.1 [CodingStandard] prohibits functions with several return places.

4.2.2.8 Coding Standards are Available (B.16)
Design and implementation follow coding standard [CodingStandard].

4.2.2.9 Coding Style/Formatting Guide (B.16)
Project-specific rules are available in [CppStyleGuide].

4.2.2.10 No Dynamic Objects (B.16)
Use of the operators new and delete is only permitted in STM State PO (Power On). After that, use of these operators will lead to a close-down of the system.

4.2.2.11 Restriction of Pointers (B.16)
The use of pointers is regulated by rules 5.5.4, 5.5.5, 5.5.8, 5.7 and 5.9.1.

4.2.2.12 Restriction of Recursion (B.16)
Recursion is only permitted in situations where the completion of the recursion can be documented.

4.2.2.13 No Unconditional Jumps (B.16)
Unconditional jumps are prohibited according to rules 7.1.1 and 7.1.2 [CodingStandard].

4.2.2.14 Analysable Programs (B.2)
Software architecture and design follow the rules for structured and object-oriented programming.

4.2.2.15 Strongly Typed Computer Language (B.57)
C++ Compiler supports type-check. Bypassing of these type-checks (e.g. by use of void pointers or preprocessor macros) must be according to [CodingStandard].

4.2.2.16 Structured Programming (B.61)
Structured programming methods are used in the software design.

4.2.2.17 Programming Language (B.16)
The Gateway software component must be implemented in C++ with the restrictions that are specified in [CodingStandard], [CppStyleGuide] and validation report [GUT-CodingStandard].

4.2.2.18 Validated Compiler (B.7)

CAD-UL C++ compiler, version V4250-TS is used for developing the Gateway software component.

4.2.2.19 Compiler Proven-In-Use (B.65)

The CAD-UL compiler and its supported tools have been used in several development projects on the SIMIS ECC and TCC platforms – consequently, it is regarded as proven-in-use.

4.2.2.20 Directories of Verified Modules and Components (B.40)

No pre-verified software modules from external source codes have been used for the Gateway software component.

4.2.2.21 Analysis of Threshold Values (B.4)

The module test must include a test of threshold values for the external interfaces of the module. There must be a test case for each threshold value.

4.2.2.22 Reaction Timing and Memory Restrictions (B.52)

A reaction timing test with special emphasis on the brake relays will be carried out in the integration phase.

4.2.2.23 Interface Test (B.37)

A module test will test the module interfaces and their threshold values.

4.2.2.24 Data Collection and Analysis (B.13)

Documents, plans and protocols developed during the project will be compiled and filed – see [PEACC+].

4.2.2.25 Object-Oriented Programming (B.68)

The Gateway software component uses object-oriented design supported by UML and the characteristics made available by the C++ programming language.

5 Messages from DK-STM

5.1 System Messages from DK-STM

DK-STM can display system messages on DMI as described below.

5.1.1 ”DK-STM: ENTER TRAIN DATA or SHUNT”

The message is used after completed shunting where the user can either enter train data or continue shunting.

5.1.2 ”DK-STM: Wait. Train Data Being Transferred”

This message is displayed in connection with transfer of train data to DK-STM.

5.2 Fault Messages from DK-STM

Fault messages from DK-STM are composed of the pre-fix “FF” followed by a three-digit integral number. The description of the fault code in question can be found in the User Manual SN655.00 Q2960.

The fault message will be displayed on DMI using the following format:

ATC: FFxxx Pzzzz

zzzz being the position of the last passed balise.

The fault messages can be read on various interfaces – these are described in detail together with the list of faults in the User Manual.

6 List of Components

The following listed physical components form part of DK-STM.

6.1 SIMIS TCC 19" Rack

Component no. S25160-C2001-A1-.*.
Manufacturer: Siemens AG

6.2 SIMIS TCC VE5A, CPU

Component no. S25391-B90-X23-.*.
Manufacturer: Siemens AG

6.3 SIMIS TCC SERIO5

Component no. S25391-B94-A2-.*.
Manufacturer: Siemens AG

6.4 SIMIS TCC PROFI5

Component no. S25391-B98-A2-.*.
Manufacturer: Siemens AG

6.5 SIMIS TCC SRAUS5-24V

Component no. S25391-B92-A2-.*.
Manufacturer: Siemens AG

6.6 SIMIS TCC SRAUS5-110V

Component no. S25391-B92-A24-.*.
Manufacturer: Siemens AG

6.7 SIMIS TCC TASSE5

Component no. S25391-B111-A2-.*.
Manufacturer: Siemens AG

6.8 SIMIS TCC ÜBGEN5

Component no. S25391-B112-A2-.*.
Manufacturer: Siemens AG

6.9 SIMIS TCC SV5, 24V

Component no. S25515-B4003-A3
Manufacturer: Siemens AG

6.10 SIMIS TCC SV5, 110V

Component no. S25515-B4003-A4
Manufacturer: Siemens AG