

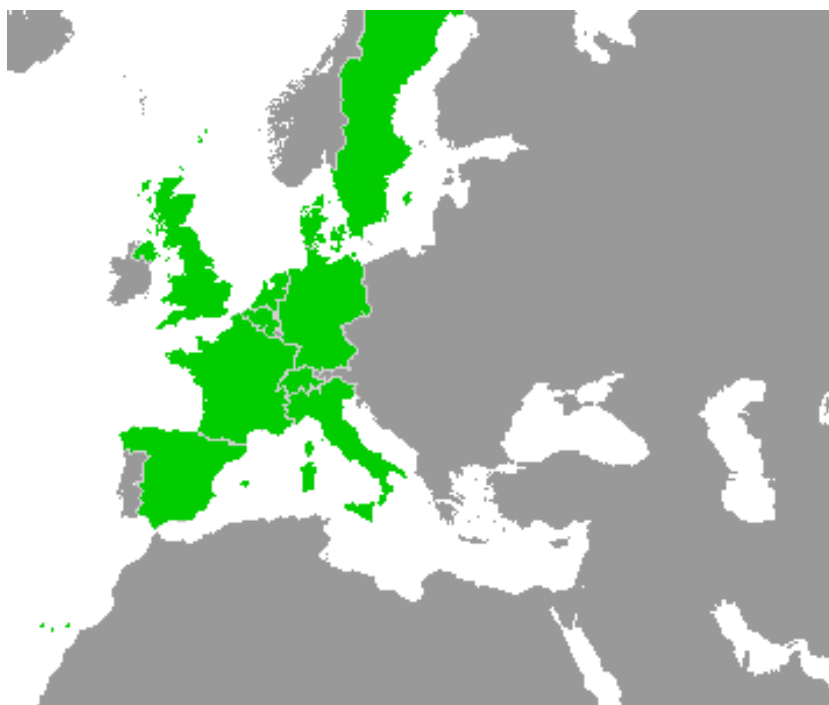
Work-Package 2: Requirements

## Methods and tools benchmarking methodology

### WP2 D2.5

David Mentre, Stanislas Pinte, Guillaume Pottier and WP2 participants

March 2012





# Methods and tools benchmarking methodology

## WP2 D2.5

David Mentre

Mitsubishi Electric R&D Centre Europe

Stanislas Pinte

ERTMS Solution

Guillaume Pottier

SNCF

WP2 participants

OpenETCS

## Requirements

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.



**Abstract:** This document is the deliverable of the WP2 D2.5 task, it defines the subset of SRS SUBSET-026 that should be used to evaluate formal modelling tools.

**Disclaimer:** This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

<http://creativecommons.org/licenses/by-sa/3.0/>

Document information	
Work Package	WP2
Deliverable ID or doc. ref.	D2.5
Document title	Methods and tools benchmarking methodology
Document version	01.00.00
Document authors (org.)	Guillaume Pottier (SNCF)

Review information	
Last version reviewed	00.00.00
Main reviewers	David Mentre, Stanislas Pinte, Marielle Petit-Doche, Guillaume Pottier

Approbation			
	Name	Role	Date
Written by	Guillaume Pottier	WP2-D2.5 Sub-Task Leader	
Approved by	Gilles Dalmas	WP2 leader	

Document evolution			
Version	Date	Author(s)	Justification
00.00.00	14/12/12	D. Mentre	Document creation
01.00.00	15/03/13	G. Pottier	Final version

# Table of Contents

<b>Figures and Tables.....</b>	<b>v</b>
<b>1 Introduction.....</b>	<b>1</b>
<b>2 Reference documents.....</b>	<b>2</b>
<b>3 Glossary .....</b>	<b>3</b>
<b>4 Content of the benchmarking.....</b>	<b>4</b>
4.1 Modelisation aspect.....	4
4.1.1 State machines .....	4
4.1.2 Time-outs .....	4
4.1.3 Arithmetics and Braking curves.....	4
4.1.4 Truth Tables and Logical Statements.....	5
4.1.5 Data structure .....	5
4.2 Proof aspect .....	6
4.2.1 §3.5.3 Establishing a communication session .....	6
4.2.2 §4.6.2 Transitions Table.....	6
4.2.3 §5.9 Procedure On-Sight.....	6
<b>5 Methodology of the benchmarking and role of WP7 .....</b>	<b>8</b>
<b>Appendix A: ERTMS/ETCS Language .....</b>	<b>9</b>
A.1 §3.5.3 Establishing a communication session .....	9
A.2 §5.9 Procedure On-Sight .....	9
A.3 §3.13 Braking curves .....	10
A.4 §4.6.2 and 4.6.3 Transition table .....	12
A.5 §4.8.3.2 From National System X .....	12
A.6 §3.6.3.2 Location, Continuous Profile Data and Non-Continuous Profile Data .....	12
A.7 §3.8.3 Structure of Movement Authority and [Pleaseinsertintopreamble]3.8.5 Update of Move- ment Authority .....	13
A.8 §3.11.3 Static Speed Profile and §3.11.12 Gradients .....	13
A.9 §8.7.2 Movement Authority message .....	13

# Figures and Tables

**Figures**

Figure 1. FTA of Kernel 19..... 7

**Tables**





# 1 Introduction

The purpose of this document is to define the methodology for the methods and tools benchmarking activities.

WP2 D2.1 has shown that several methods and tools are available to make the formal model of the On Board Unit in WP3. In order to evaluate them in WP7, WP2.D2.5 need to define a representative part of the SUBSET-026 that would be modelled by each candidate, therefore allowing comparing the tools on the same basis.

A formal model is composed of two different aspects:

- the modelisation of functionalities in a non ambiguous language/semantics (allowing refinements to the code or code generation), that we will call the *modelisation* aspect;
- the proofs of safety properties, that we will call the *proof* aspect.

For the modelisation aspect, the idea is to cover all the different means of description needed for SUBSET-026 in order to highlight the strong points and weak points of a potential language/semantic. Moreover, there is the need of having a sufficient and self content part of a functionality for the proof aspect in order to verify the proof capability of the method/tool.

This document defines only which fonctionnalities and safety requirements should be modelled for the benchmark. The criterias for the evaluation of methods and tools are not gathered in this document. For this, refer to others WP2 deliverables.

## 2 Reference documents

**SUBSET-026 3.3.0** — *System Requirement Specification*

**SUBSET-058 3.0.0** — *STM Application layer*

**SUBSET-091 3.2.0** — *Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2*

## 3 Glossary

**EBD** Emergency Brake Deceleration curve

**EBI** Emergency Brake Intervention curve

**EOA** End Of movement Authority

**FLOI** First Line Of Intervention

**FS** Full Supervision mode

**FTA** Fault Tree Analysis

**IS** ISolated mode

**MA** Movement Authority

**MRDT** Most Restrictive Displayed Target

**MRSP** Most Restrictive Speed Profile

**OBU** On Board Unit

**OS** On Sight mode

**SB** Stand By mode

**SH** SHunting mode

**SRS** System Requirement Specification

**STM** Specific Transmission Module

**TSR** Tempory Speed Restriction

**WP** Work Package

## 4 Content of the benchmarking

### 4.1 Modelisation aspect

The following paragraphs of SUBSET-026 are representative of the diversity of means of description used in the SRS and should be used in the benchmark. These paragraphs are divided into two sections: a high priority one that should be modelled first and a lower priority that should be modelled if time permits.

In Appendix A, there is a list of standardised variables for each SRS paragraph chosen for the benchmark. It will facilitate the review of the different models.

#### 4.1.1 State machines

The modelisation of state charts will indicate if the review of this modelisation is easy or not according to the SRS. There are several state charts in chapter 5 and some of them are huge, especially the first one "start of mission".

**HIGH PRIORITY §5.9 Procedure On-Sight** State chart which contains a timer and is not too long.

#### 4.1.2 Time-outs

The OBU is in interface with the trackside and it means that time-outs management is needed.

**HIGH PRIORITY §3.5.3 Establishing a communication session**

#### 4.1.3 Arithmetics and Braking curves

The OBU must calculate several braking curves to determine if it will not exceed the safe speed / distance. These curves are defined in baseline 3, chapter 3.13 of SUBSET-026. Braking curves represent a big challenge for formal models. Indeed it is not always possible to do it in the high level modelisation language, but rather in low level language like C or ADA. The following examples take into account different aspects of this problematic.

**HIGH PRIORITY §3.13.4 (Acceleration / Deceleration due to gradients)**

**HIGH PRIORITY §3.13.6.2 Emergency brake** and more particularly:

- §3.13.6.2.1.3 (calculation of  $A_{safe}$ , function of  $V$  and  $d$ , depending on the gradient profile, braking models of the train, several correction factors etc; this is the basis of the EBD curve, see Figure 38)

**HIGH PRIORITY §3.13.7 Determination of Most Restrictive Speed Profile (MRSP)** Combine for example several TSR and LX restrictions

**HIGH PRIORITY §3.13.8.3 Emergency Brake Deceleration curves (EBD)**

**HIGH PRIORITY §3.13.9.3.3.9 Computation of d\_FLOI, using d\_SBI2\_MREBDT** (MREBDT: Most Restrictive Target amongst the EBD based targets)

**HIGH PRIORITY §3.13.9.4 Release speed supervision limits** and more particularly:

- §3.13.9.4.7 (computation of different release speed supervision limits)
- §3.13.9.4.8 (computation of the most restrictive value at the Trip location related to the EOA, amongst several EBI supervision limits)
- 3.13.9.4.8.2 (iterative computation of the release speed)
- §3.13.9.4.9 (using of the most restrictive MRSP value instead of the release speed)

**HIGH PRIORITY §3.13.10.4.2 Calculation of the MRDT**

#### 4.1.4 Truth Tables and Logical Statements

SUBSET-026 can be considered as a tool box and there is also a lot of modes / information / functionality available. All these possibilities are combined into big truth tables representing hundreds of cases. The modelisation of these tables will indicate if the review of this modelisation is easy or not according to the SRS.

**HIGH PRIORITY §4.6.2 (Transitions Table) and §4.6.3 (Transitions Condition table)** Only transitions:

1. from SB to SH
2. from SB to FS
3. from SB to IS

Having transitions at different priority level is important to look at priority issues and exclusion issues at the same priority level.

**Low priority §4.8.3.2 From National System X (through STM interface)** Model a small table.

#### 4.1.5 Data structure

SUBSET-026 defines the format and content of messages for ERTMS/ETCS functions. The ERTMS/ETCS language (refer to SUBSET-026 chapter 7 and 8) is used for transmitting information over the radio, balise and loop airgaps and the STM interface. It is based on variables, packets, messages and telegrams.

**Low priority §3.6.3.2 Location, Continuous Profile Data and Non-Continuous Profile Data**  
Example of complex generic data structure.

**Low priority §3.8.3 Structure of Movement Authority and §3.8.5 Update of Movement Authority**  
Example of complex procedure, with complex data.

**Low priority §3.11.3 Static Speed Profile and §3.11.12 Gradients** Example of data structure, referring to §3.6.3.2 and used by §3.13.4.

**Low priority §8.7.2 Movement Authority message** This includes reference to Packet 15 (§7.4.2.4). That would be a perfect use case for tools able to model things down to bit level.

## 4.2 Proof aspect

From the previous list, only §3.5.3 (Establishing a communication session), §4.6.2 (Transitions Table) and §5.9 (Procedure On-Sight) would be considered in this section. The others are not sufficiently self content.

Since the safety process is not precisely defined at the moment, **the following paragraph must not be used as reference for the future safety activities. There is no guarantee of completeness or correctness.**

The objective is only to give some examples of safety requirements that can be used for testing the proof capability of a tool / method. SUBSET-091 will then be considered as the basis.

IMPORTANT NOTE: In SUBSET-026, all the requirements related to one function are not gathered in the same paragraph. They are in different sections. So there is a risk that it can be difficult or impossible to prove some safety requirements because a part of the proof needs more information than what is specified in the chosen paragraph.

### 4.2.1 §3.5.3 Establishing a communication session

Safety requirements will be proposed according to the following SUBSET-091 items:

KERNEL-5 Radio link supervision function failure

KERNEL-6 Manage communication session failure

Without trying a FTA or FMECA approach, a simple property comes directly in mind:

**PROPERTY\_3.5.3\_01** OBU shall never have two different communication sessions established at the same time (with the same RBC or with two different)

### 4.2.2 §4.6.2 Transitions Table

Safety requirements will be proposed according to the following SUBSET-091 item:

KERNEL-27 Incorrect System Data

Most of the safety behavior is yielded by the model itself and it is difficult to produce a set of declarative properties, and to avoid paraphrase. In Isolation mode, OBU has no more responsibility and is isolated from the brakes, we can consider that the transition to or from this mode is safety relevant.

**PROPERTY\_4.6.2\_01** OBU shall never enter in isolated mode if not requested by the driver

**PROPERTY\_4.6.2\_02** OBU shall never leave Isolated mode (no transition from Isolation is specified)

### 4.2.3 §5.9 Procedure On-Sight

Safety requirements will be proposed according to the following SUBSET-091 item:

KERNEL-19 Failure of train trip supervision in OS, LS and FS

Let's try a FTA approach (*Figure 1*).

The result is three safety requirements.

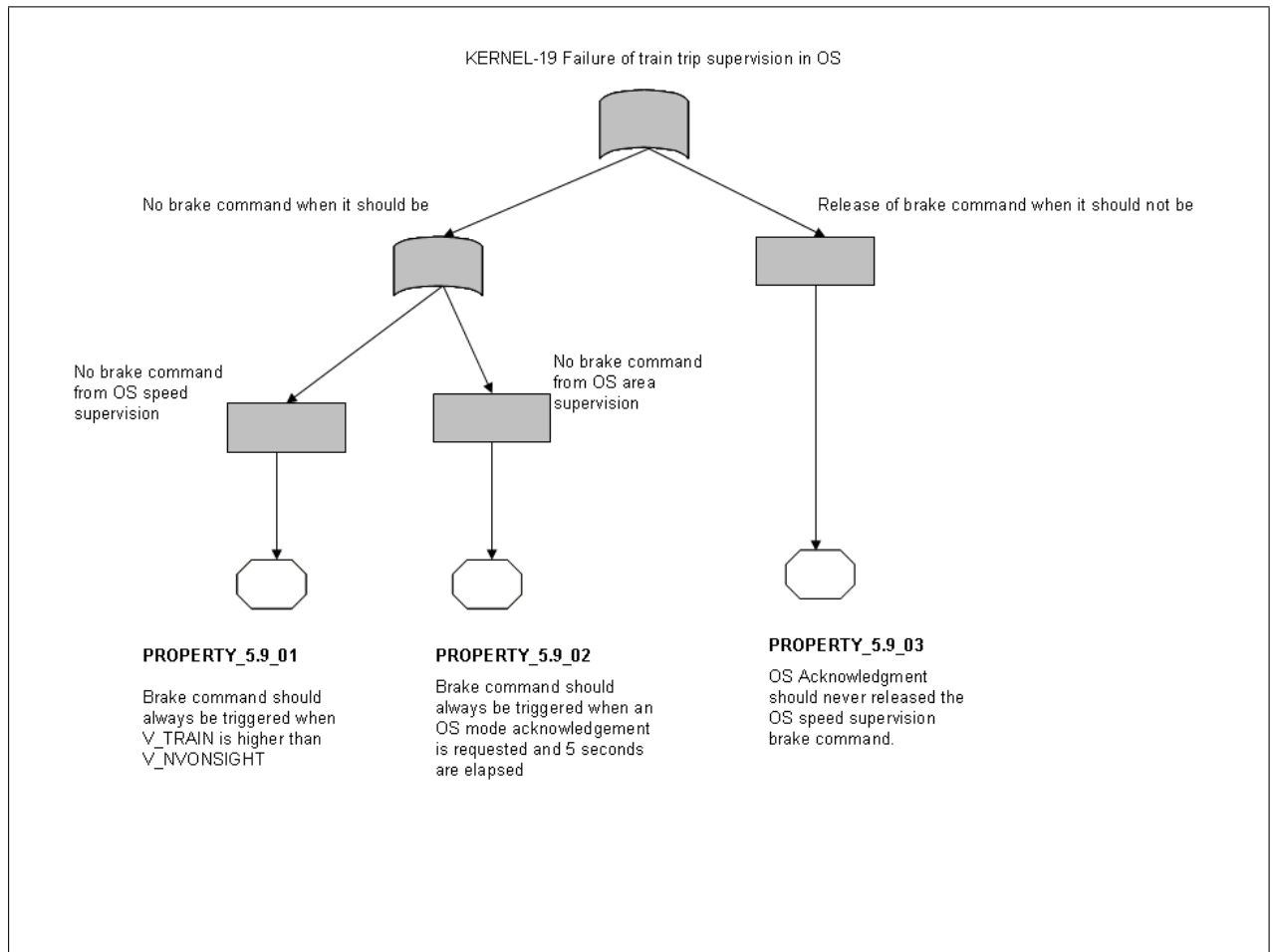


Figure 1. FTA of Kernel 19

**PROPERTY\_5.9\_01** Brake command should always be triggered when V\_TRAIN is higher than V\_NVONSIGHT

**PROPERTY\_5.9\_02** Brake command should always be triggered when an OS mode acknowledgement is requested and 5 seconds are elapsed

**PROPERTY\_5.9\_03** OS Acknowledgment should never released the OS speed supervision brake command.

## 5 Methodology of the benchmarking and role of WP7

WP2 is in charge of the definition of the benchmark (this document).

WP7 is in charge of the realisation of the benchmark. The evaluation matrix will be created by WP7, based on the deliverables of WP2.

The evaluation shall be done by independant persons from those who has done the modelisation and from the provider of the means or tools.



## Appendix A: ERTMS/ETCS Language

The purpose of this appendix is to propose common variables / packets / messages for the models.

*Variables shall be used to encode single data values. Variables cannot be split in minor units. The whole variable has one type (meaning)*

*Packets are multiple variables grouped into a single unit, with a defined internal structure.*

*A message (Euroradio/Euroloop) or telegram (Eurobalise) shall be composed of one Header, when needed, a predefined set of variables (only for Radio), when needed, a predefined set of Packets (only for Radio), optional Packets as needed by application.*

All the variables are not defined since it could depend on modelisation choices (especially internal variables of the OBU which are not defined in the SUBSET-026). It is also mainly focussed on chapter 7 and 8 of SUBSET-026.

The following lists are surely not complete but it is a good basis.

### A.1 §3.5.3 Establishing a communication session

**Packet Train to Track :** SUBSET-026 §7.4.3.3 Packet number 3 Onboard telephone numbers

**Message Train to Track :** SUBSET-026 §8.6.13 Message 155 Initiation of a communication session

**Message Train to Track :** SUBSET-026 §8.6.14 Message 155 Termination of a communication session

**Message Train to Track :** SUBSET-026 §8.6.17 Message 159 Session established

**Packet Track to Train :** SUBSET-026 §7.4.2.1 Packet number 2 System Version order

**Packet Track to Train :** SUBSET-026 §7.4.2.10 Packet number 42 Session Management

**Packet Track to Train :** SUBSET-026 §7.4.2.11.1 Packet number 45 Radio Network registration

**Packet Track to Train :** SUBSET-026 §7.4.2.27 Packet number 131 RBC transition order

**Packet Track to Train :** SUBSET-026 §7.4.2.37.1 Packet number 143 Session Management with neighbouring Radio Infill Unit

**Message Track to Train :** SUBSET-026 §8.7.12 Message 32 RBC/RIU System Version

**Message Track to Train :** SUBSET-026 §8.7.16 Message 38 Initiation of a communication session

**Message Track to Train :** SUBSET-026 §8.7.17 Message 39 Acknowledgement of termination of a communication session

### A.2 §5.9 Procedure On-Sight

**Variable :** SUBSET-026 §7.5.1.72 M\_MODE

**Variable :** SUBSET-026 §7.5.1.65 M\_LEVEL

**Variable :** SUBSET-026 §7.5.1.162 V\_NVONSIGHT

**Variable :** SUBSET-026 §7.5.1.172 V\_TRAIN

**Message Train to Track :** SUBSET-026 §8.6.7 Message 146 Acknowledgement

**Message Train to Track :** SUBSET-026 §8.6.9 Message 149 Track ahead free granted

**Packet Track to Train :** SUBSET-026 §7.4.2.26 Packet number 80 Mode profile

**Packet Track to Train :** SUBSET-026 §7.4.2.26.2 Packet number 90 Track Ahead Free up to level 2/3 transition location

**Message Track to Train :** SUBSET-026 §8.7.14 Message 34 Track Ahead Free request

### **A.3 §3.13 Braking curves**

**Variable :** SUBSET-026 §7.5.0.1 A\_NVMAXREDADH1

**Variable :** SUBSET-026 §7.5.0.2 A\_NVMAXREDADH2

**Variable :** SUBSET-026 §7.5.0.3 A\_NVMAXREDADH3

**Variable :** SUBSET-026 §7.5.0.4 A\_NVP12

**Variable :** SUBSET-026 §7.5.0.5 A\_NVP23

**Variable :** SUBSET-026 §7.5.1.1 D\_ADHESION

**Variable :** SUBSET-026 §7.5.1.4 D\_DP

**Variable :** SUBSET-026 §7.5.1.13 D\_LRBG

**Variable :** SUBSET-026 §7.5.1.19.1 D\_PBD

**Variable :** SUBSET-026 §7.5.1.19.2 D\_PBDSR

**Variable :** SUBSET-026 §7.5.1.37 G\_A

**Variable :** SUBSET-026 §7.5.1.37.1 G\_PBDSR

**Variable :** SUBSET-026 §7.5.1.38 G\_TSR

**Variable :** SUBSET-026 §7.5.1.48.1 L\_NVKRINT

**Variable :** SUBSET-026 §7.5.1.49.1 L\_PBDSR

**Variable :** SUBSET-026 §7.5.1.56 L\_TRAIN

**Variable :** SUBSET-026 §7.5.1.57 L\_TRAININT

**Variable :** SUBSET-026 §7.5.1.65 M\_LEVEL

**Variable :** SUBSET-026 §7.5.1.73.1 M\_NVAVADH

**Variable :** SUBSET-026 §7.5.1.75.1 M\_NVEBCL

**Variable :** SUBSET-026 §7.5.1.75.2 M\_NVKRINT

**Variable :** SUBSET-026 §7.5.1.75.3 M\_NVKTINT

**Variable :** SUBSET-026 §7.5.1.75.4 M\_NVKVINT

**Variable :** SUBSET-026 §7.5.1.110 Q\_GDIR

**Variable :** SUBSET-026 §7.5.1.115 Q\_LOCACC

**Variable :** SUBSET-026 §7.5.1.123.2 Q\_NVINHSMICPERM

**Variable :** SUBSET-026 §7.5.1.123.3 Q\_NVKINT

**Variable :** SUBSET-026 §7.5.1.123.4 Q\_NVKVINTSET

**Variable :** SUBSET-026 §7.5.1.126.1 Q\_PBDSR

**Variable :** SUBSET-026 §7.5.1.155 V\_AXLELOAD

**Variable :** SUBSET-026 §7.5.1.156 V\_DIFF

**Variable :** SUBSET-026 §7.5.1.157 V\_LOA

**Variable :** SUBSET-026 §7.5.1.157.1 V\_LX

**Variable :** SUBSET-026 §7.5.1.158 V\_MAIN

**Variable :** SUBSET-026 §7.5.1.159 V\_MAMODE

**Variable :** SUBSET-026 §7.5.1.160 V\_MAXTRAIN

**Variable :** SUBSET-026 §7.5.1.161 V\_NVALLOWOVTRP

**Variable :** SUBSET-026 §7.5.1.161.1 V\_NVKVINT

**Variable :** SUBSET-026 §7.5.1.161.2 V\_NVLIMSUPERV

**Variable :** SUBSET-026 §7.5.1.162 V\_NVONSIGHT

**Variable :** SUBSET-026 §7.5.1.163 V\_NVSUPOVTRP

**Variable :** SUBSET-026 §7.5.1.164 V\_NVREL

**Variable :** SUBSET-026 §7.5.1.165 V\_NVSHUNT

**Variable :** SUBSET-026 §7.5.1.166 V\_NVSTFF

**Variable :** SUBSET-026 §7.5.1.167 V\_NVUNFIT

**Variable :** SUBSET-026 §7.5.1.168 V\_RELEASEDP

**Variable :** SUBSET-026 §7.5.1.169 V\_RELEASEOL

**Variable :** SUBSET-026 §7.5.1.170 V\_REVERSE

**Variable :** SUBSET-026 §7.5.1.171 V\_STATIC

**Variable :** SUBSET-026 §7.5.1.172 V\_TRAIN

**Variable :** SUBSET-026 §7.5.1.173 V\_TSR

**Packet Track to Train :** SUBSET-026 §7.4.2.6 Packet number 21 Gradient Profile

**Packet Track to Train :** SUBSET-026 §7.4.2.37 Packet number 141 Default Gradient for Temporary Speed Restriction

#### A.4 §4.6.2 and 4.6.3 Transition table

**Variable :** SUBSET-026 §7.5.1.13 D\_LRBG

**Variable :** SUBSET-026 §7.5.1.72 M\_MODE

**Variable :** SUBSET-026 §7.5.1.65 M\_LEVEL

**Variable :** SUBSET-026 §7.5.1.172 V\_TRAIN

**Message Train to Track :** SUBSET-026 §8.6.2 Message 130 Request for Shunting

**Message Train to Track :** SUBSET-026 §8.6.7 Message 146 Acknowledgement

**Packet Track to Train :** SUBSET-026 §7.4.2.3 Packet number 12 Level 1 Movement Authority

**Packet Track to Train :** SUBSET-026 §7.4.2.4 Packet number 15 Level 2/3 Movement Authority

**Packet Track to Train :** SUBSET-026 §7.4.2.6 Packet number 21 Gradient Profile

**Packet Track to Train :** SUBSET-026 §7.4.2.7 Packet number 27 International Static Speed Profile

**Packet Track to Train :** SUBSET-026 §7.4.2.37 Packet number 141 Default Gradient for Temporary Speed Restriction

**Packet Track to Train :** SUBSET-026 §7.4.2.26 Packet number 80 Mode profile

**Message Track to Train :** SUBSET-026 §8.7.2 Message 3 Movement Authority

**Message Track to Train :** SUBSET-026 §8.7.10 Message 27 SH Refused

**Message Track to Train :** SUBSET-026 §8.7.11 Message 28 SH Authorised

#### A.5 §4.8.3.2 From National System X

**Variable :** SUBSET-026 §7.5.1.65 M\_LEVEL

**Packet Track to Train :** SUBSET-026 §7.4.2.9 Packet Number 41 Level Transition Order

**Packet STM to Train :** SUBSET-058 §7.2.8 Packet STM-16 Transition variables STM max speed from STM

**Packet STM to Train) :** SUBSET-058 §7.2.9 Packet STM-17 Transition variables STM system speed and distance from STM

#### A.6 §3.6.3.2 Location, Continuous Profile Data and Non-Continuous Profile Data

**Variable :** SUBSET-026 §7.5.1.13 D\_LRBG

**Variable :** SUBSET-026 §7.5.1.22 D\_REF

**Variable :** SUBSET-026 §7.5.1.90 NID\_LRBG

**Variable :** SUBSET-026 §7.5.1.94 NID\_PRVLRBG

**Variable :** SUBSET-026 §7.5.1.103 Q\_DIR

**Variable :** SUBSET-026 §7.5.1.104 Q\_DIRLRBG

**Variable :** SUBSET-026 §7.5.1.105 Q\_DIRTRAIN

**Variable :** SUBSET-026 §7.5.1.106 Q\_DLRBG

**Packet Track to Train :** SUBSET-026 §7.4.2.5 Packet number 16 Repositioning Information

**Message Track to Train :** SUBSET-026 §8.7.13 Message 33 MA with Shifted Location Reference

#### **A.7 §3.8.3 Structure of Movement Authority and §3.8.5 Update of Movement Authority**

**Packet Track to Train :** SUBSET-026 §7.4.2.3 Packet number 12 Level 1 Movement Authority

**Packet Track to Train :** SUBSET-026 §7.4.2.4 Packet number 15 Level 2/3 Movement Authority

**Packet Track to Train :** SUBSET-026 §7.4.2.32 Packet number 136 Infill location reference

**Message Track to Train :** SUBSET-026 §8.7.2 Message 3 Movement Authority

**Message Track to Train :** SUBSET-026 §8.7.13 Message 33 MA with Shifted Location Reference

**Message Track to Train :** SUBSET-026 §8.7.15 Message 37 Infill MA

#### **A.8 §3.11.3 Static Speed Profile and §3.11.12 Gradients**

**Packet Track to Train :** SUBSET-026 §7.4.2.6 Packet number 21 Gradient Profile

**Packet Track to Train :** SUBSET-026 §7.4.2.7 Packet number 27 International Static Speed Profile

**Packet Track to Train :** SUBSET-026 §7.4.2.37 Packet number 141 Default Gradient for Temporary Speed Restriction

#### **A.9 §8.7.2 Movement Authority message**

**Packet Track to Train :** SUBSET-026 §7.4.2.4 Packet number 15 Level 2/3 Movement Authority

**Message Track to Train :** SUBSET-026 §8.7.2 Message 3 Movement Authority