



WP4 – 1st Workshop on Safety Assessment OpenETCS Status System Analysis

supported by:



Federal Ministry
of Education
and Research



Région de
Bruxelles-
Capitale



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

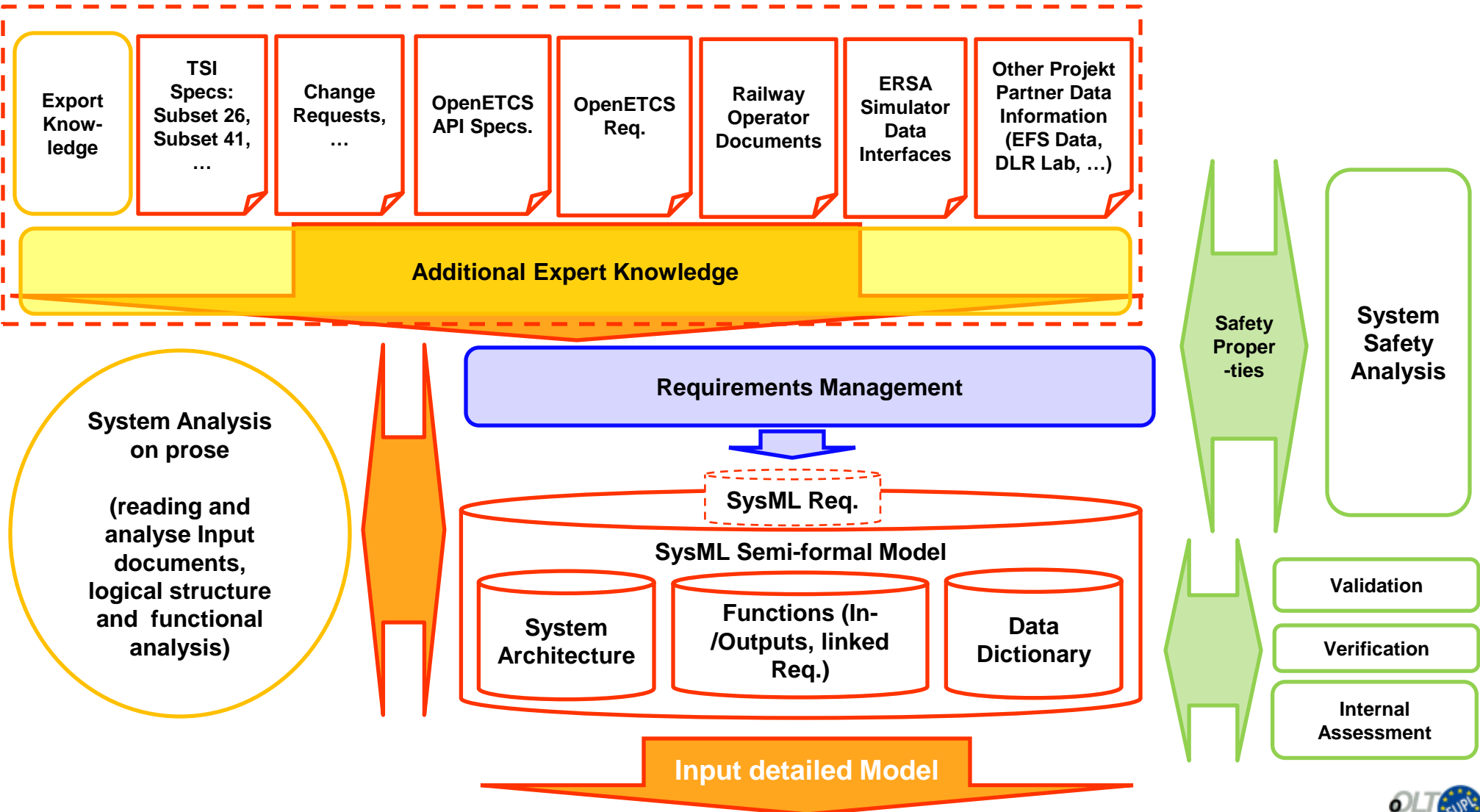
openETCS@ITEA2 Project

Jan Welte, TU-BS

Nürnberg, 18.02.2014

Development Process and Toolchain

System Analysis Process



List of functions

- System Experts agreed on list of 52 Kernel function in 7 areas
 - DataPreparation
 - GATC TRAINBORNE SUB SYSTEM
 - Provide automatic train protection
 - Active_and_Manage_train_protection
 - Manage_mode_and_level_and_procedures_and_ancillary_functions
 - Manage_procedures
 - Perform_ancillary_functions

Number	Name	Block/Function	Complexity	Group
1	DataPreparation	B		
1.1	Board_External Interface	F		
1.2	GATC TRAINBORNE SUB SYSTEM	B		
1.2.1	Filter_information_from_ERTMS_trackside (including linking)	F	3	Group 1
1.3	Provide automatic train protection	B		
1.3.1	Manage_STMs	F	3	
1.3.2	Determine_train_location_information	F	3	Group 4
1.3.3	Control_route_suitability	F	1	Group 1
1.3.4	Manage_track_conditions	F	2	Group 2
2	Ensure_train_protection	B		
2.1	Manage_reception_of_MA_information	F	2	Group 3
2.2	Manage TSR	F	1	Group 2
2.3	Manage_Speed_Supervision_Inputs	F	2	
2.4	Active_and_Manage_train_protection	B		
2.4.1	Activate_train_protection_in_FS	F	3	
2.4.2	Activate_train_protection_in_OS	F	3	
2.4.3	Activate_train_protection_in_LS	F	3	
2.4.4	Activate_train_protection_in_SR	F	2	
2.4.5	Activate_train_protection_in_UN	F	2	
2.4.6	Activate_train_protection_in_SH	F	2	
2.4.7	Activate_train_protection_in_TR	F	2	
2.4.8	Activate_train_protection_in_SF	F	1	
2.4.9	Activate_train_protection_in_SB	F	2	
2.4.10	Activate_train_protection_in_PT	F	2	
2.4.11	Activate_train_protection_in_RV	F	2	
2.4.12	Activate_train_protection_in_IS	F	1	
2.4.13	Perform_train_protection	F	3	
2.4.14	Perform_train_protection_related_actions	F	3	
2.4.15	Activate_train_protection_in_SN	F	2	
2.4.16	Activate_train_protection_in_PS	F	2	
2.4.17	Activate_train_protection_in_NP	F	1	
2.3	Manage_emergency_stop_messages	F	2	
3	Manage_mode_and_level_and_procedures_and_ancillary_functions	B	3	
3.1	compute_mode	F	2	

SSRS Task Force

First System Analysis Work

	A	B	C	D	E	F	G	H	I	J	K
1	Number	Name	Parent	Allocation	Input	Output	Internal	Requirement	Source	Safety	Definition
2	Integer	T_Text	T_Function	T_System	T_Variable (optional)	T_Variable (optional)	T_Variable (optional)	T_Requirement (optional)		Boolean	T_Definition
5		WRITE_BT _INFO		(Kernel)		BTM_INFO		210 useful bits for the short format 830 useful bits for the long format	(036-4.3.2.2)		(kernel basic SW function)
6		BAD_BALIS E received		(Kernel)		BAD_BALISE					(kernel basic SW function)
8	1	Perform Eurobalise decoding		Kernel	BTM_INFO	Telegram_from_eurobalise					This function shall decode any telegram which is received from an eurobalise to extract useful bits
9					BAD_BALISE			The reasons for which a telegram shall be considered as not correctly coded are the following : (a) a CRC error is detected			
10								(b) at least one variable of the telegram has a spare value, an invalid value or an undefined value	3.16.1.1		
11								(c) the effective length of at least a packet of the telegram is not equal to the length indicated in the header of the packet (L_PACKET)			
12								d) There is a packet not authorised for the media			
								(e) the "end of information" packet 255			

Proof of Concept for System Analysis

Structured Analysis of single functions

- Understand functional specification
- Determine Input/ Output
- Allocate and Refine Requirements

System Analysis

To clarify the specifications of Subset 26 additional documents have been derived by the partners

- Collect specific uses cases
- Present needed calculations
- Name variables

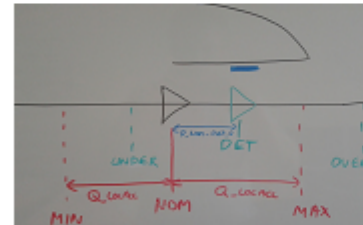
Maximum distance between nominal BG location and the nominal BG detected ($D_{nom-det_X}$):

The maximum distance between the detected BG location and the nominal BG location is determined by:

- The accuracy with which the BG is installed in the track. This inaccuracy shall be assumed to be equal to or less than Q_{LOCACC} which is given from track side (or is available as a default value: $Q_{NVLOCACC}$ or default NV). For BG "X" this inaccuracy is referred to as " Q_{LOCACC_X} ".
- The accuracy with which the train borne equipment is able to determine the center of the BG. This inaccuracy shall be calculated. The calculation is out of the scope of this document. The result for the detection of BG "X" is stored in the variable " $DetectionAcc_X$ ".

The maximum distance between the detected BG location of BG "X" (" $X_{detection}$ ") and the nominal location of BG "X" (" X_{nom} ") shall be calculated and stored in " $D_{nom-det_X}$ ":

- $Dmin_nom-det_X$: The lowest possible value of $X_{detection} - X_{nom}$, thus a negative value if the BG can be detected in rear of the nominal position of the BG "X"
- $Dmax_nom-det_X$: The highest possible value of $X_{detection} - X_{nom}$, thus a positive value if the BG can be detected in advance of the nominal position of the BG "X"



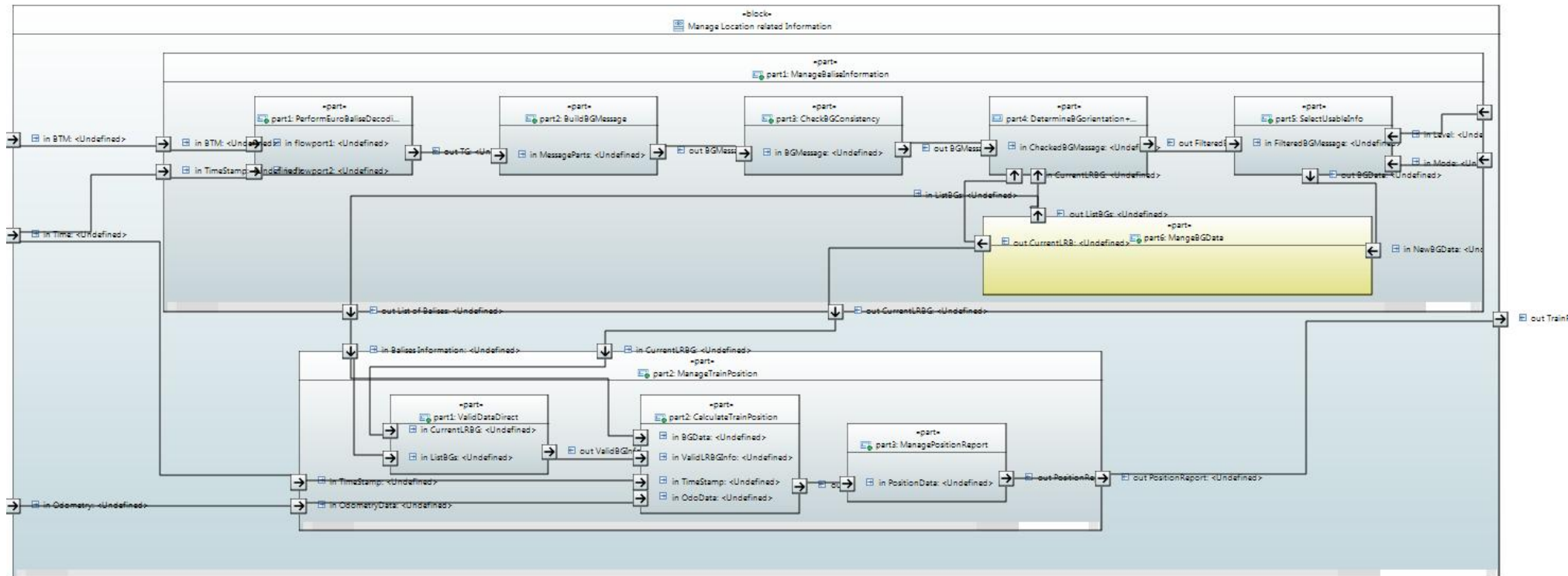
Picture showing the spread from the detection location, replace the left side picture with one without under and over.....

Measured distance as given by the odometer

Train Position and Locations, version 0.0.13, 10-2-2014

SSRS Task Force

First Model approach



SysML (Papyrus) Architecture Model

- Train Location Functionality
 - Reading Balise Message
 - Manage Location Information

Questions or Discussion



Technische
Universität
Braunschweig

Institut für Verkehrssicherheit und Automatisierungstechnik iVA

Prof. Dr.-Ing. Dr. h.c. mult. E. Schnieder



Jan Welte

TU Braunschweig

Institute for Traffic Safety and Automation Engineering

welte@iva.ing.tu-bs.de