Proceedings of the European Safety and Reliability Conference, ESREL 2008, and 17th SRA-Europe, 22-25 September 2008, Valencia, Spain, Volume 4. CRC Press, Taylor & Francis Group: pp. 3163-3169

Availability assessment of ALSTOM's safety-relevant trainborne odometry sub-system

B.B. Stamenković
Swiss Federal Railways SBB, I-ST-ZB, RAMS, Bollwerk 10, 3000 Berne 65, Switzerland

P. Dersin
ALSTOM Transport Information Solutions, 23-25 Avenue Morane Saulnier, 92360 Meudon-la-Forêt Cedex, France

ABSTRACT: ALSTOM's trainborne ERTMS/ETCS solutions have been applied world wide by many new railways projects. The heart of that system is the European Vital Computer (EVC), controlling all safety relevant functionalities.

In order to achieve the best safety-related and availability performances of safety-related vital functionalities, the 2-out-of-3 protection architecture is applied for the three EVC basic channels. The failures of at least 2-out-of-3 EVC channels, as well as the failures of some vital safety-related trainborne functionalities, such as the functionality of the odometry sub-system, result in spurious emergency brake application.

The basic concepts of the availability modelling and assessment of the odometry functionality are presented for two different configurations of the odometry sub-system based on the use of one radar, one accelerometer and two wheel sensors, each of them using either three or only two sensor cells.

1 INTRODUCTION

In the framework of the ambitious Swiss Federal Railways (SBB)'s SA-NBS (Signalling and Automation Systems on the Mattstetten-Rothrist section of the Zurich-Berne high-speed line) project (including 11 types of vehicles) and the New Pendolino ETR610 project, a total of 482 vehicles have been retrofitted with ALSTOM's trainborne ERTMS/ETCS solutions (total of 540 EVCs).

The reliability and availability requirements related to significant failures are based on the spurious Emergency Brake (EB) application.

The availability assessment is based on the application of the RBD technique. In the first phase, the needed RBDs have been developed for each of the needed vital safety-related trainborne functionalities. In the next phase, equivalent RBDs have been generated covering all vital safety-related trainborne functionalities in order to estimate the resulting reliability and availability indices.

The reliability and availability modelling and assessment of the important odometry functionality have been carried out by joint SBB and ALSTOM efforts.

1.1 *Abbreviations*

ATC	Automatic Train Control
ERTMS	European Rail Traffic Management System
EB	Emergency Brake
ETCS	European Train Control System
EVC	European Vital Computer
MTBF	Mean operating Time Between Failures
MTBSF	Mean operating Time Between Service (System) Failures
MTTR	Mean Time To Restoration/Recovery
RBD	Reliability Block Diagram
SA-NBS	Signalling and Automation Systems on New Swiss High Speed Line (Mattstetten-Rothrist)
SBB AG	Schweizerische Bundesbahnen AG (Swiss Federal Railway company)
λ	Failure rate
μ	Restoration/recovery (repair) rate

2 SPURIOUS EMERGENCY BRAKE (EB) APPLICATION

There are some small differences in the applications of ALSTOM's ATC trainborne sub-system by different projects. But in all of them the ATC trainborne sub-system spuriously applies the EB if at least one the following events occurs:

- at least one of the two emergency brakes voters is spuriously opened in the EVC section;
- at least 2-out-of-3 (2oo3) EVC channels are faulty, and then inhibited;
- the transmission eurobalise sub-system fails;
- the connection to the train (backplane) fails; and/or
- the odometry sub-system functionality fails.

The basic availability modelling approach is based on the generation of appropriate RBDs relating to each of the specified functionalities, and then to the generation of an equivalent RBD covering all these functionalities.

In generating the different RBDs it appears that one of the key RBDs needed for the availability modelling of the spurious emergency brake application is related to odometry sub-system functionality. Hence a special attention will be given in the present paper to availability modelling of odometry sub-system functionality.

3 AVAILABILITY MODELLING OF THE ODOMETRY SUB-SYSTEM FUNCTIONALITY

3.1 *Architecture of the odometry sub-system*

Motion sensors that are used by the odometry sub-system are of the following three types:

- wheel sensors (WSs);
- radar (R); and
- accelerometer (AC).

There are a few different possible configurations. In the SA-NBS and ETR610 projects, the vehicles are equipped with two wheel sensors (WSs); where each of the WS consists of three WS cells (WSCs). Each WSC is able to give two square wave signals with a frequency proportional to the rotation speed.

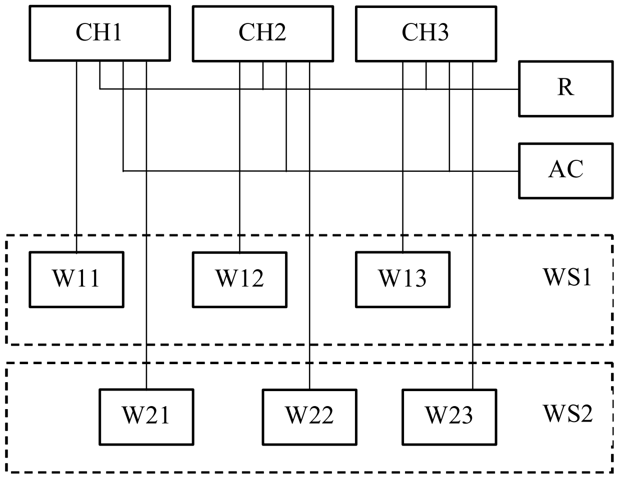

Figure 1. General odometry sub-system configuration; CHj (j = 1, 2, 3) is the basic EVC channel consisting of a few PBAs; radar (R); accelerometer (AC); wheel sensors WSi (i = 1, 2); generating wheel sensor cell signals Wij , with i and j denoting, respectively, the i-th wheel sensor and the j-th channel CHj (i = 1, 2; j = 1, 2, 3).

Starting from these signals — speed, distance and direction of the movement can be calculated.

Each WSC gives two square wave signals. The signals of the same WSC have a predefined phase shift to allow the detection of the direction of rotation.

The general sensor input configuration is shown in Figure 1:

- there is one radar (R), one accelerometer (AC) and two wheel sensors (WSs);
- the R and the AC are connected to all three odometry boards (SDMUs) of the EVC; and
- the wheel sensor WSi generate signals Wij for the odometry board SDMUj of the j-th channel CHj (i = 1, 2; j = 1, 2, 3).

3.2 *The protection architecture of the three EVC channels*

The most important safety relevant functionalities of the EVC are realised using three channels in a 2oo3 protection architecture. Each of the three channels (CHj; j = 1, 2, 3) is realised by using a few different PBAs of the EVC. One of these PBAs is the odometry board $SDMU_j$ (j = 1, 2, 3).

3.3 *The basic odometry algorithm*

In (ALSTOM 2006, section 5.3.1.2), actions after the validity checking of sensor inputs relating to the isolation of some channels are described. The basic odometry algorithm is based on the following three statements:

(A) each channel must have at least one of its two wheel sensor cells valid for that channel to remain active;
(B) if all channels are active, there must be at least 7 out of 12 inputs in a valid status; and
(C) if only two channels are active, there must be at least 5 out of 8 inputs in a valid status.

3.4 *Availability modelling — an approximation*

According to Figure 1, each channel CHj (j = 1, 2, 3) is (over the corresponding odometry board SDMUj) supplied with 4 sensor signals (wheel sensor, radar and accelerometer), and a 2oo3 protection architecture is applied for the three channels.

The requirement (A) implies that two sensor cells have to be in an (n-1) out of n protection architecture ($n \geq 2$).

The RBD1 shown in Figure 2 will be used for the availability assessment of odometry sub-system functionalities.

Let us consider RBD1 on Figure 2, where a 3oo4 protection architecture is used for the sensor inputs. The functionality represented by RBD1 fails if at least one of the following cases has occurred:

1. Internal failure of at least two CHj (j = 1, 2, 3);
2. Failure of the R and of the AC (6 failed sensor inputs);
3. Failure of the AC and at least two wheel sensor inputs of one WSi (i = 1, 2); or at least one W1i and W2j, (i, j = 1, 2, 3 with $i \neq j$) (5 failed sensor inputs);
4. Failure of the R and at least two wheel sensor inputs of one WSi (i = 1, 2); or at least one W1i and W2j, (i, j = 1, 2, 3 with $i \neq j$) (5 failed sensor inputs);
5. Failure of at least two pairs (W1j, W2j) for j = 1, 2, 3 (4 failed sensor inputs); or
6. Internal failure of one CHj (j = 1, 2, 3) and

   6.1 Failure of the R and at least one wheel sensor input, which is not part of the failed channel (3 failed sensor inputs);
   6.2 Failure of the AC and at least one wheel sensor input, which is not part of the failed channel (3 failed sensor inputs); or
   6.3 Failure of at least one pair (W1j, W2j) for j = 1, 2, 3, which is not part of the failed channel (2 failed sensor inputs).

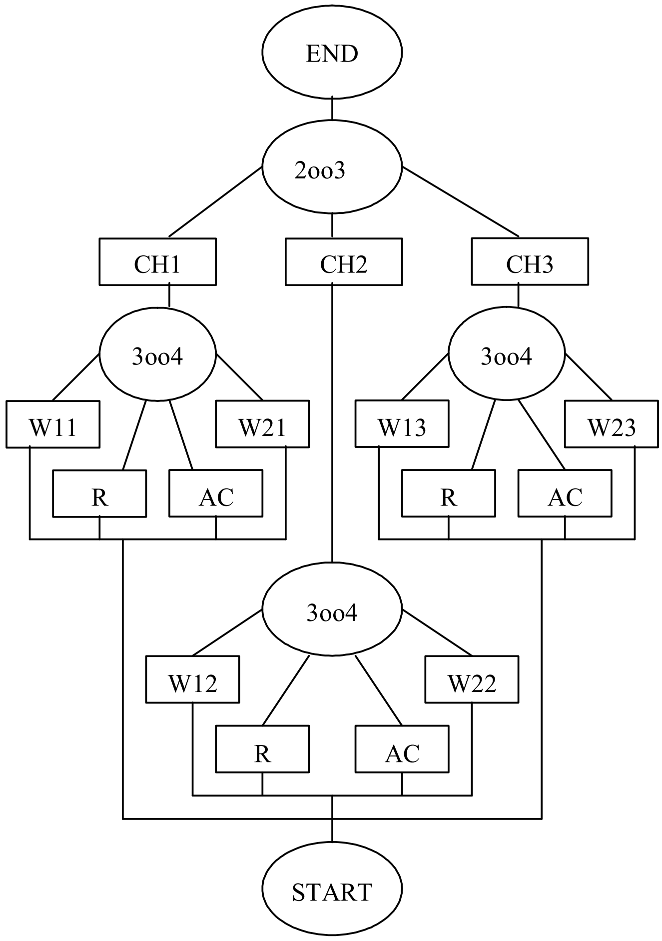

Figure 2. RBD1 used for the reliability and availability assessment of the odometry sub-system functionality, with Wij (i = 1, 2; j = 1, 2, 3) being the input signal for the j-th channel of the i-th wheel sensor WSi; R and A being radar and accelerometer, respectively.

The comparison of condition (B) with statements 1-5, and condition (C) with statement 6, respectively, leads to the conclusion that conditions 1-6 are stronger then the requirements (B) and (C), i.e. MTBSF(odometry sub-system) $\geq$ MTBSF(RBD1). Hence, if trainborne MTBSF requirement MTBSF(trainborne) is satisfied with MTBSF(RBD1), it will also be satisfied with MTBSF(odometry sub-system).

The initial RBD1 contains elements, such as R and AC, where each of them appears three times in the RBD1. Hence, in this case the Key Item Method can be applied (Birolini 2007, section 2.3.1), where the following four cases have to be considered:

i. R and AC are good (operate failure free);

ii. R is wrong (failed) and AC is good;

iii. R is good and AC is wrong; and

iv. R and AC are wrong.

At this point some needed relations to reliability and availability modelling are recalled.

Let us consider system S, containing elements E_1 and E_2. Denote with $A(E_i)$ the availability and with $A(\bar{E}_i)$ the unavailability of element E_i ($i = 1, 2$); and let $A(S/E_i)$ $[A(S/\bar{E}_i)]$ denotes the conditional availability that the system is available under condition that element E_i is good (operates failure free) [wrong (failed)]. Then, by assuming that the elements are independent (each element operates, fails and is repaired independently of every other element) and that each of them is characterised by constant failure rate (λ), constant repair rate (μ), and one separate repair crew, one has:

$$A(S) = A(E_1)A(S/E_1) + A(\bar{E}_1)A(S/\bar{E}_1), \quad (1)$$

$$A(S/E_1) = A(E_2)A(S/E_1/E_2) + A(\bar{E}_2)A(S/E_1/\bar{E}_2), \quad (2)$$

$$A(S/\bar{E}_1) = A(E_2)A(S/\bar{E}_1/E_2) + A(\bar{E}_2)A(S/\bar{E}_1/\bar{E}_2). \quad (3)$$

Inserting Equations 2 and 3 into Equation 1 one has:

$$\begin{aligned} A(S) &= A(E_1)[A(E_2)A(S/E_1/E_2) + A(\bar{E}_2)A(S/E_1/\bar{E}_2)] \\ &\quad + A(\bar{E}_1)[A(E_2)A(S/\bar{E}_1/E_2) + A(\bar{E}_2)A(S/\bar{E}_1/\bar{E}_2)] \\ &= A(E_1)A(E_2)A(S/E_1/E_2) \\ &\quad + A(E_1)A(\bar{E}_2)A(S/E_1/\bar{E}_2) \\ &\quad + A(\bar{E}_1)A(E_2)A(S/\bar{E}_1/E_2) \\ &\quad + A(\bar{E}_1)A(\bar{E}_2)A(S/\bar{E}_1/\bar{E}_2). \end{aligned} \quad (4)$$

Let

$$E_1 = R,\ E_2 = AC, \quad (5)$$

$$A(\bar{E}_i) = 1 - A(E_i)\ (i = 1, 2). \quad (6)$$

Then

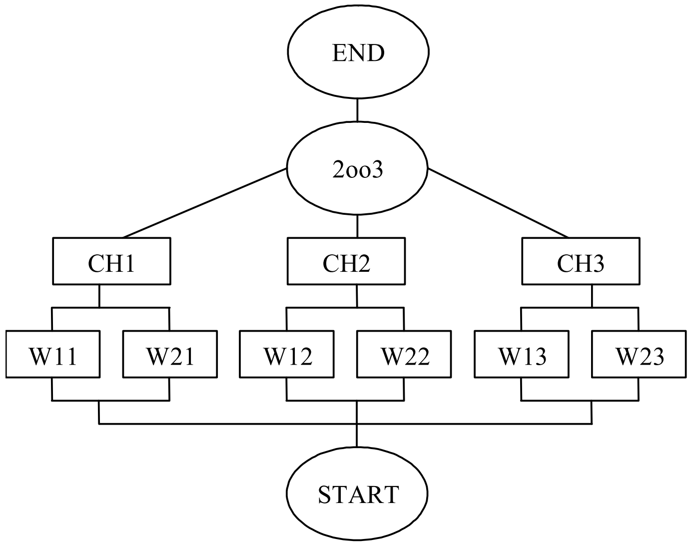

Figure 3. RBD2 of the odometry sensors generated from RBD1 for the case when R and AC are good (operate failure free); with Wij being signals of the wheel sensor WSi for the j-th channel CHj (i = 1, 2; j = 1, 2, 3).

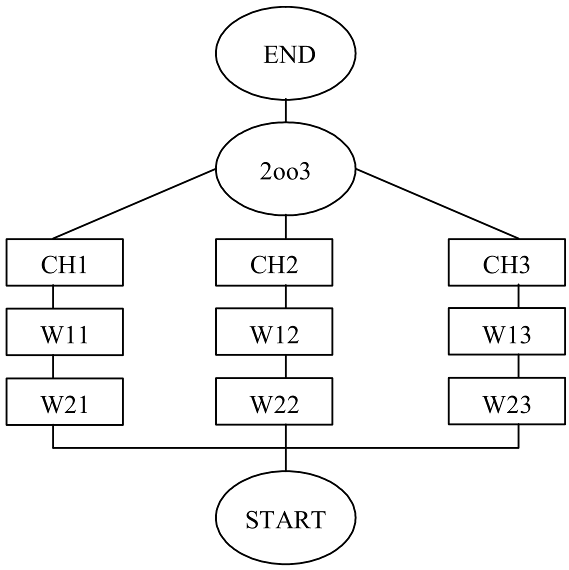

Figure 4. RBD3 of the odometry sensors generated from RBD1 for the case when either (i) R is good (operates failure free) and AC is wrong (failed); or (ii) R is wrong and AC is good; with Wij (i = 1, 2; j = 1, 2, 3) being the signal input of the wheel sensor WSi for the j-th channel CHj (i = 1, 2; j = 1, 2, 3).

$$\begin{aligned} &A(S/E_1/E_2) = A(RBD2), \\ &A(S/E_1/\bar{E}_2) = A(S/\bar{E}_1/E_2) = A(RBD3), \\ &A(S/\bar{E}_1/\bar{E}_2) = 0, \end{aligned} \quad (7)$$

and

$$A(S) = A(R)A(AC)A(RBD2) + \{A(R)[1 - A(AC)] + A(AC)[1 - A(R)]\}A(RBD3), \quad (8)$$

where:

- RBD2, shown in Figure 3, is derived from RBD1 for the case when both R and AC are good (operate failure free);
- RBD3, shown in Figure 4, is derived from RBD1 for the case when either (i) R is wrong (failed) and AC is good (operates failure free); or (ii) R is good and C is wrong; and
- In the case when both R and AC are wrong the associated asymptotic availability of the system is equal to zero.

For the system level, one has

$$A(S) = A_S = \mu_S/(\mu_S + \lambda_S) = 1/(\lambda_S/\mu_S + 1), \quad (9)$$

giving

$$\lambda_S = \mu_S(1/A_S - 1), \text{ MTBSF} = \text{MTBF}_S = 1/\lambda_S. \quad (10)$$

Therefore, the procedure for the estimation of λ_S is as follows:

- Calculate $A(S) = A_S$ according to Equation 8;
- Assume that in the worst case $\mu_S = 1/(9h)$; and
- Calculate λ_S and/or MTBF_S using Equation 10.

3.5 *RAM figures for two different wheel sensor cells configurations*

The basic two different wheel sensor cells configurations are specified in Table 1. Configuration (a) (ALSTOM-Italy 2007) corresponds to Figure 1, with Wij = WSCij (i = 1, 2; j = 1, 2, 3), and configuration (b) (ALSTOM-Belgium 2007) is shown in Figure 5.

3.6 *Configuration (a): Project ETR610*

In this case one has the following expressions for the availabilities associated with RBD2 and RBD3:

$$\begin{aligned} A(RBD2) &= A(RBD2a) \\ &= A(CH1)A(CH2)[A(W11) + A(W21) \\ &\quad - A(W11)A(W21)][A(W12) \\ &\quad + A(W22) - A(W12)A(W22)] \\ &\quad + A(CH1)A(CH3)[A(W11) + A(W21) \\ &\quad - A(W11)A(W21)][A(W13) \\ &\quad + A(W23) - A(W13)A(W23)] \\ &\quad + A(CH2)A(CH3)[A(W12) + A(W22) \\ &\quad - A(W12)A(W22)][A(W13) \\ &\quad + A(W23) - A(W13)A(W23)] \\ &\quad - 2A(CH1)A(CH2)A(CH3)[A(W11) \\ &\quad + A(W21) - A(W11)A(W21)][A(W12) \\ &\quad + A(W22) - A(W12)A(W22)][A(W13) \\ &\quad + A(W23) - A(W13)A(W23)], \end{aligned} \quad (11)$$

$$\begin{aligned} A(RBD3) &= A(RBD3a) \\ &= A(CH1)A(CH2)A(W11)A(W21) \\ &\quad \times A(W12)A(W22) + A(CH1)A(CH3) \\ &\quad \times A(W11)A(W21)A(W13)A(W23) \\ &\quad + A(CH2)A(CH3)A(W12)A(W22) \\ &\quad \times A(W13)A(W23) - 2A(CH1) \\ &\quad \times A(CH2)A(CH3)A(W11)A(W21) \\ &\quad \times A(W12)A(W22)A(W13)A(W23), \end{aligned} \quad (12)$$

where Wij = WSCij (i = 1, 2; j = 1, 2, 3).

Let us denote with $\lambda(X)$, $\mu(X)$ and $A(X) = \mu(X)/[\mu(X) + \lambda(X)]$ the failure rate, the repair rate and the availability, respectively, of the element X, with X = Wij, WSCij, CHj, R, AC (i = 1, 2; j = 1, 2, 3). Then, by assuming

$$\lambda(CHj) = \lambda(CH), \ \mu(CHj) = \mu(CH) \ (j = 1, 2, 3), \quad (13)$$

$$\lambda(Wij) = \lambda(WSC) = \lambda(W),$$

$$\mu(Wij) = \mu(WSC) = \mu(W) \ (i = 1, 2; j = 1, 2, 3), \quad (14)$$

one has

$$A(RBD2a) = A_1^2 (3 - 2A_1), \quad (15)$$

with

$$A_1 = A(W)[2 - A(W)]A(CH), \quad (16)$$

Table 1. Reliability and availability modelling of the odometry sub-system for two different wheel sensor cells configurations

Wheel sensor cell	Channel inputs (Wij)					
	Channel 1		Channel 2		Channel 3	
	W11	W21	W12	W22	W13	W23
Configuration (a): Project ETR610 — Three independent wheel sensor cells WSCij are used by each of the wheel sensors WSi (i = 1, 2; j = 1, 2, 3)						
WSC11	x					
WSC12			x			
WSC13					x	
WSC21		x				
WSC22				x		
WSC23						x
Configuration (b): Project SA-NBS — Only two wheel sensor cells WSCij are used by the wheel sensor WSi (i = 1, 2; j = 1, 2) to realize 6 wheel sensor inputs						
WSC11					x	
WSC12	x		x			
WSC21				x		x
WSC22		x				

$$A(RBD3a) = A_2^2\,(3 - 2A_2), \qquad (17)$$

with

$$A_2 = A^2(W)A(CH). \qquad (18)$$

3.7 *Configuration (b): Project SA-NBS*

In this case one obtains the following expressions:

$$\begin{aligned}
A(RBD2) &= A(RBD2b)\\
&= A(CH1)A(CH2)[A(WSC12)\\
&\quad + A(WSC22)A(WSC21)\\
&\quad - A(WSC12)A(WSC22)A(WSC21)]\\
&\quad + A(CH1)A(CH3)[A(WSC12)\\
&\quad + A(WSC22) - A(WSC12)A(WSC22)]\\
&\quad \times [A(WSC11) + A(WSC21)\\
&\quad - A(WSC11)A(WSC21)\\
&\quad + A(CH2)A(CH3)[A(WSC21)\\
&\quad + A(WSC12)A(WSC11)\\
&\quad - A(WSC12)A(WSC11)A(WSC21)]\\
&\quad - 2A(CH1)A(CH2)A(CH3)\{A(WSC12)\\
&\quad \times A(WSC21) + A(WSC12)A(WSC11)\\
&\quad + A(WSC22)A(WSC21) - A(WSC12)\\
&\quad \times A(WSC21)[A(WSC11)\\
&\quad + A(WSC22)]\},
\end{aligned} \qquad (19)$$

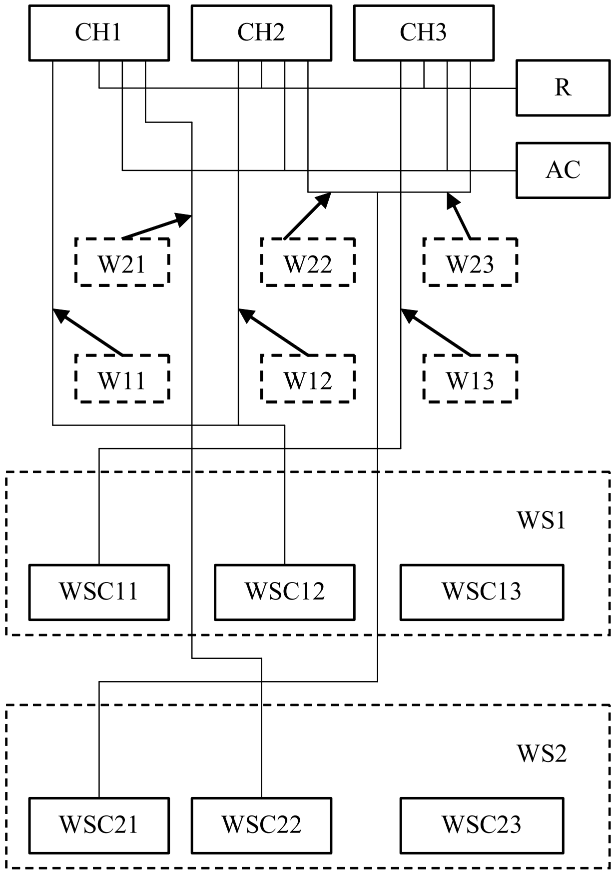

Figure 5: SA-NBS Project — Odometry sub-system; Wheel sensors configuration (b); CHj (j = 1, 2, 3) is the basic channel consisting of a few PBAs; radar (R); accelerometer (AC); wheel sensors WSi (i = 1, 2); wheel sensor cells WSCij, being the j-th cell of wheel sensor WSi (i = 1, 2; j = 1, 2, 3); and Wij (i = 1, 2; j = 1, 2, 3) being the wheel sensor input signals to the odometry boards SDMUj (j = 1, 2, 3).

$$\begin{aligned}
A(RBD3) &= A(RBD3b)\\
&= A(WSC12)A(WSC21)[A(CH1)\\
&\quad \times A(CH2)A(WSC22) + A(CH1)\\
&\quad \times A(CH3)A(WSC22)A(WSC11)\\
&\quad + A(CH2)A(CH3)A(WSC11)\\
&\quad - 2A(CH1)A(CH2)A(CH3)\\
&\quad \times A(WSC22)A(WSC11)].
\end{aligned} \qquad (20)$$

For CHi = CH and WSCij = W one has

$$A(RBD2b) = A(CH)^2 A(W)\{2[1 + A(W) - A(W)^2] + A(W)[2 - A(W)]^2 - 2A(CH)A(W)[3 - 2A(W)]\}, \quad (21)$$

$$A(RBD3b) = A(CH)^2 A(W)^3 [2+A(W) - 2A(CH)A(W)]. \quad (22)$$

4 RESULTS

The MTBSF assessments of odometry sub-system functionality for two different configurations of wheel sensor cells are given in Table 2.

Table 2. Odometry sub-system MTBSF assessment; MTBSF as a function of MTBF(WSC); MTBSF comparison for two configuration variants of wheel sensor cells applied in the ETR610 and SA-NBS projects.

Item	Failure rate [1E-06/h]	MTBF [h]	MTTR [h]	A
R	6.02	166,113	9	0.999945823
AC	12.5	80,000	9	0.999887513
CH	29.435	33,973	9	0.999735155

MTBSF comparison: K = MTBSFa/MTBSFb

1/MTBF(WSC) [1/h]	ETR610 Project MTBSFa [h]	SA-NBS Project MTBSFb [h]	K
0.01 (*)	55,921	8053	6.9
0.0001 (*)	40,935,322	17,338,251	2.4
2.68E-06 (*)	41,570,373	40,083,764	1.037

(*) test value; the real MTBF(WSC) values have been omitted for confidentiality reasons

5 CONCLUSIONS

Availability assessment has been carried out for two different configurations of ALSTOM's odometry sub-system applied in two ALSTOM trainborne ERTMS/ETCS projects.

The RBD technique and the key item method have been used by availability modelling of the structure in which some elements have appeared several times in the RBDs, although physically there is only one such element in the considered item.

The availability assessment shows that ETR610 architecture of odometry sub-system is preferable from a service availability point of view.

The presented availability modelling method, assumptions, approximations, assessment and obtained results can be applied by the availability modelling of different, project specific ALSTOM's ERTMS / ETCS trainborne sub-systems with different configurations of odometry sub-system.

REFERENCES

ALSTOM, 2006. *Speed and Distance Measurement Unit – General Technical Design, document GATC/BSI/DE-SIGN /0374.*

ALSTOM-Belgium, 2007. *Reliability and Availability Assessment of the Trainborne Sub-system, document SA-NBS_ BSI_ RAMS _0242.*

ALSTOM-Italy, 2007. SSB-*AV new Pendolino — Preliminary RAM Report, document 270501CXXRS002.*

Birolini, A. 2007. *Reliability Engineering — Theory and Practice*, *5th edition.* Springer.