A Multiformalism Modular Approach to ERTMS/ETCS Failure Modelling

Article *in* International Journal of Reliability Quality and Safety Engineering · February 2014

DOI: 10.1142/S0218539314500016

5 authors, including:

Francesco Flammini
Mälardalen University
234 PUBLICATIONS **1,744** CITATIONS
SEE PROFILE

Stefano Marrone
Università degli Studi della Campania "Luigi Vanvitelli
116 PUBLICATIONS **1,075** CITATIONS
SEE PROFILE

Mauro Iacono
Università degli Studi della Campania "Luigi Vanvitelli
131 PUBLICATIONS **1,527** CITATIONS
SEE PROFILE

Nicola Mazzocca
University of Naples Federico II
308 PUBLICATIONS **3,227** CITATIONS
SEE PROFILE

International Journal of Reliability, Quality and Safety Engineering
Vol. 21, No. 1 (2014) 1450001 (29 pages)

DOI: 10.1142/S0218539314500016

World Scientific
www.worldscientific.com

A MULTIFORMALISM MODULAR APPROACH TO ERTMS/ETCS FAILURE MODELING

FRANCESCO FLAMMINI

Innovation and Competitiveness Unit, AnsaldoSTS
via Argine, 425, 80147, Naples, Italy
francesco.flammini@ansaldo-sts.com

STEFANO MARRONE

Dip. di Matematica e Fisica, Seconda Universitá di Napoli
via Lincoln, 5, 81100, Caserta, Italy
stefano.marrone@unina2.it

MAURO IACONO

Dip. di Studi Politici, Seconda Universitá di Napoli
Viale Ellittico, 31, 81100, Caserta, Italy
mauro.iacono@unina2.it

NICOLA MAZZOCCA* and VALERIA VITTORINI†

Dip. di Ingegneria Elettrica e Tecnologie dell'Informazione
Universitá di Napoli "Federico II"
Via Claudio, 21, 80125, Naples, Italy
**nicola.mazzocca@unina.it*
†*valeria.vittorini@unina.it*

Received 20 October 2011
Revised 4 October 2013
Accepted 23 December 2013
Published 20 January 2014

European Railway Traffic Management System/European Train Control System (ERTMS/ETCS) is a recent standard aimed at improving performance, safety and interoperability of modern railways. In order to be compliant to ERTMS/ETCS, a railway signalling system must meet strict nonfunctional requirements on system level failure modes. In this paper, a multiformalism model is employed to perform an availability analysis of an ERTMS/ETCS reference architecture at early phases of its development cycle. At this aim, a bottom-up analysis is performed from subsystem failure models (expressed by means of Generalized Stochastic Petri Nets, Fault Trees and Repairable Fault Trees) up to the overall system model. The modular approach, here used, allows to evaluate the influence of basic design parameters on the probability of system-level failure modes and demonstrates that system availability is within the bound required by the ERTMS/ETCS specification. The results show that the multiformalism modeling

approach helps to cope with complexity, eases the verification of availability requirements and can be successfully applied to the analysis of complex critical systems.

Keywords: RAM requirements; ERTMS/ETCS; system design; nonfunctional properties; multiformalism modeling.

1. Introduction

The goal of railway signalling is the safe movement of trains and the optimal regulation of traffic flows. The European Railway Traffic Management System (ERTMS) is a recent standard for the interoperability of the European railway signalling systems. The ERTMS specifications are mandatory on Trans European Network Routes. ERTMS includes: (a) the European Train Control System (ETCS), that is responsible for the safe movement of the trains[1]; (b) the European Traffic Management Layer (ETML), that is a traffic management system in charge of optimizing the flow over the network, and (c) a Global System for Mobile Communications for Railway (GSM-R) radio communication system. Different implementations of ERTMS are possible, since the standard states *part* of its structure and *some* of the system parameters.

Several scientific papers present in the literature study automatic train protection/control systems[2–6]; at the best of our knowledge, few public results are available about system reliability and availability analysis of ERTMS/ETCS. A hierarchical approach is described to develop a Colored Petri Net model that represents the on-board and trackside subsystem (TCS) behaviors and their interactions with the environment.[7] A cause-consequence model of ERTMS/ETCS (Level 2) for risk forecasting is developed according to a systematic assessment framework.[8] A methodology for hazard analysis is presented and applied to the ERTMS/ETCS system.[9] Another major contribution comes from the research conducted on modeling and analysis of GSM-R network by means of Deterministic Stochastic Petri Nets (DSPNs).[10,11] In particular, the EuroRadio protocol is the subject of further studies based on semi-formal techniques.[12] Some of our previous works focused attention on multiformalism as a way to model and analyze railway systems.[13,14] In this paper, we address the development of a failure model of ERTMS/ETCS systems according to a modeling approach based on the combined use of more formal modeling and analysis techniques. As the ongoing deployment of ERTMS/ETCS is entrusted by different pilot projects overall Europe, in this work we consider a reference architecture. In order to evaluate availability requirements and perform a sensitivity analysis on this architecture, a set of parameters is chosen. Here, we address two classes of possible failures stated by the specification: immobilizing failures (IFs) and service failures (SFs). Since the safety analysis of the system is out of the scope of this work, in the following we refer to RAM (Reliability, Availability, Maintainability) requirements.[15,16]

The development of a failure model of an ERTMS/ETCS system is a hard task, since its architecture is very complex. The complexity is due to many factors including the physical distribution of system components, the high number of interacting

subsystems, the computing performances affecting the overall system availability, and the criticality of the communications. The purpose of this paper is to provide a modular approach to the availability analysis of ERTMS/ETCS; the approach also allows to evaluate the influence of basic design parameters on the probability of the occurrence of system-level failure modes.

In order to cope with complexity, the modeling approach used in this paper is based on compositional and multiformalism techniques. In the first approach a model consists of several submodels tied together by appropriate rules and composition operators: in order to provide appropriate methods for solving submodels and aggregating results, composition techniques and operators definition are necessary. A comprehensive survey of these approaches is present in the scientific literature.[17] On the other hand multiformalism is based on the usage of heterogeneous submodels: it reduces the complexity of the analysis with respect to the effort needed if the system would be approached as a whole and allows to use different modeling languages to describe different subsystems.[18–21] The choice of the most proper languages is made according to the overall nonfunctional property to evaluate (failure probability, in this case). A complementary approach deals with the generation of formal models from high-level specifications: the scientific community has explored this topic and several research papers are present in the literature; some of them focus on railway systems.[22–24]

The use of modeling formalisms enables a rigorous analysis of the system even at early stages of its development process. In this paper Fault Trees (FT),[25] Repairable Fault Trees (RFT)[26] and Generalized Stochastic Petri Nets (GSPN) are combined using Bayesian Networks (BN). A FT model is used to perform a reliability analysis of subsystems that cannot be easily repaired on-line; a RFT model is used to perform an availability analysis (including the modeling of maintenance aspects); a GSPN model is used to cope with timing issues. The results of the analysis of these sub-models are then integrated into a global BN model of the system in order to obtain the overall probability of SFs and IFs. A sensitivity analysis is performed in order to support design decisions in ERTMS/ETCS systems development.

The choice of the formalisms used in this paper is based on the results of the comparison among some formalisms (i.e., FT, BN and GSPN) in terms of modeling power and solving efficiency[27]; moreover, a demonstration of the power of the RFT is available.[26]

Due to confidentiality reasons, the analysis has been done with real scale data of the system, i.e., data with the same magnitude of order of the real data, used to provide realistic results. Quantitative parameters have been derived from datasheets of Components Off-The-Shelf (COTS), whenever available, or according to Reliability, Availability, Maintainability and Safety (RAMS) requirements for constituents, in case of specific ERTMS/ETCS components.

The paper is organized as follows. In Sec. 2, the ERTMS/ETCS reference architecture is described. In Sec. 3, the classes of system failures and the related RAM requirements of interest are introduced. Section 4 describes the modeling approach

and the models used for the analysis of ERTMS/ETCS. In Sec. 5, the models are evaluated and the results of the sensitivity analysis are discussed. Finally, Sec. 6 contains closing remarks and directions for future works.

2. ERTMS/ETCS Reference Architecture

The mission of ERTMS/ETCS is to ensure railway interoperability. At this aim, it provides the specification of a traffic management and train control system that enables the transit of high speed trains through national borders. The ERTMS/ETCS standard ensures both technological compatibility among transeuropean railway networks and integration of the new signalling system with the existing national train interlocking systems (IXL). An ERTMS/ETCS system consists of heterogeneous, distributed components that are installed on the train, along the tracks and in several control centers. A reference architecture for ERTMS/ETCS systems is shown in Fig. 1. It consists of three main subsystems:

— The lineside subsystem: it is mainly responsible for providing geographical position information to the on-board subsystem (ONB);
— The ONB: it is the core of the control activities located on the train;
— The TCS: it is in charge of monitoring the movement of the trains.

The components that must be compliant with the ERTMS/ETCS specifications are shadowed in Fig. 1. Notice that the ERTMS/ETCS specifications do not address the IXL: each national railway authority is free to use proprietary (existing) solutions. Hence the analysis of IXL is out of the scope of this work and the failures due to the IXL system are not considered in the models. In the next subsections we briefly describe the components that must be compliant with the ERTMS/ETCS

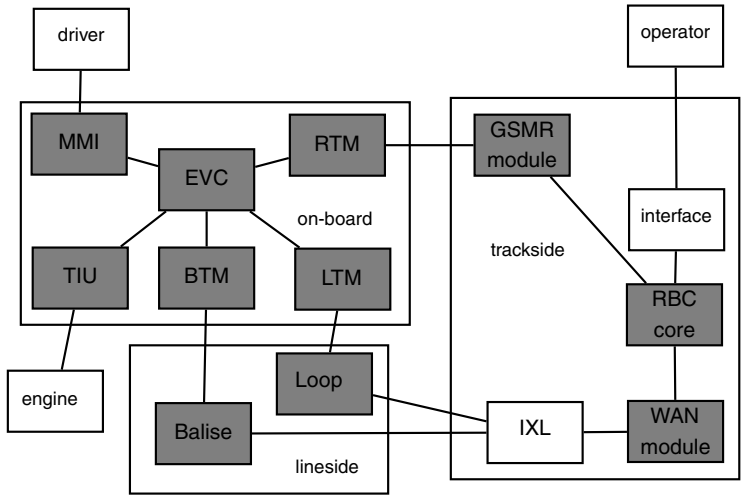

Fig. 1. ERTMS/ETCS architecture.

public specifications,[1] thus providing a more detailed description of the three subsystems and their inter-relationships.

2.1. *The lineside subsystem*

The lineside subsystem is distributed on the whole track. The communication between the on-board, trackside and lineside subsystems is provided by the following standardized mechanisms:

— *EuroBalise*: a *discontinuous* unidirectional communication system from the lineside to the ONB. It is based on *balises* which are electronic devices placed between the track lines and organized into groups of two or more of them. The balises can be used as milestones to detect the train position. They communicate the train position to the ONB and can receive information from the TCS.
— *EuroRadio*: a *continuous* communication protocol that allows the on-board and the TCSs to interact via GSM-R.
— *EuroLoop*: a straightforward extension of EuroBalise that replicates the balises messages over a longer distance to realize a *semi-continuous* signalling system.

The ERTMS/ETCS specifications identify three functional levels featuring growing complexity. They can be implemented singularly or in conjunction and mainly differ in the communication mechanisms adopted to control the trains. According to Level 1 specifications, the trains communicate with the TCS by means of signals transmitted by EuroLoop and EuroBalise. According to the Level 2 specifications, the main communication system is EuroRadio. At Level 3, train integrity is a responsibility of the on-board system allowing the removing of a track segmentation by means of track circuits (that is outside of ERTMS reference architecture): this reduce the possible outdistancing between trains improving the throughput of the railway network. Starting from the consideration that Level 2 and Level 3 represents two more cutting-edge solutions than Level 1, at this moment Level 2 is the most widespread choice between Level 2 and Level 3, according to current deployment statistics[28]; hence this paper refers to ERTMS Level 2.

2.2. *The ONB*

The ONB is mainly composed of seven components that are listed in the glossary reported in Table 1. If a dangerous condition occurs, the ONB subsystem must notify it to the driver and start the proper braking procedure.

The class diagram in Fig. 2 describes the on-board equipment in detail. *At least one back-up unit for each device is provided.* The LTM component reported in Fig. 1 is omitted here, since it is not used at Level 2. The core of the ONB is the European Vital Computer (EVC), a fail-safe computing system. EVC is in charge of supervising the train speed. A Triple Modular Redundancy (TMR) scheme is applied to obtain a fault tolerant computation, consisting of a 2-out-of-3 voting on the outputs of three CPU cards (CPU in the following).[a] Voter

Table 1. Glossary of abbreviations.

Name	Component	Description
	On-Board Subsystem (ONB)	
BTM	Balise transmission module	It reads data from balises via EuroBalise protocol
EVC	European vital computer	On-board core control system of ERTMS/ETCS
LTM	Loop transmission module	It reads data from track loop via EuroLoop protocol
MMI	Man machine interface	Interface between the ERTMS on-board system and the train driver
ODO	Odometer	It evaluates kinematic train variables (speed and position)
RTM	Radio transmission module	It receives and sends data on GSM-R network via EuroRadio protocol
TIU	Train interface unit	Interface between the ERTMS on-board system and some trainy devices
	Trackside Subsystem (TCS)	
GSM-R	GSM network for railways	Enhancement of the GSM network for railway signalling purposes
IXL	Interlocking system	It is responsible for the correct routing of trains on the railway network
RBC	Radio block center	It is responsible for the correct outdistancing between trains
WAN	Wide area network	It allows RBC-RBC and RBC-IXL communication

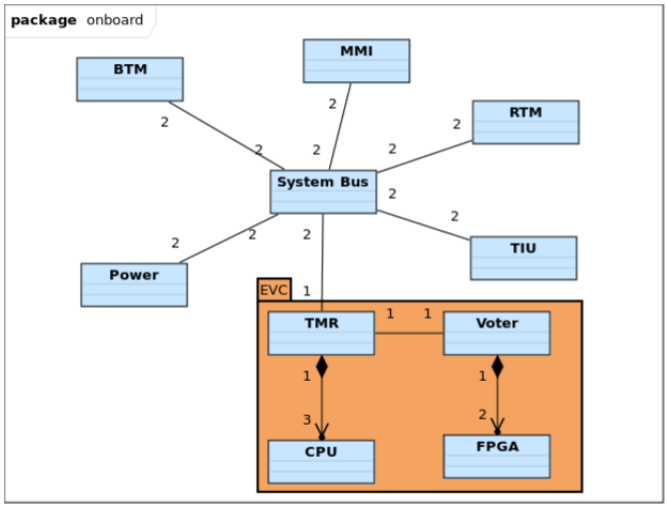

Fig. 2. Class diagram of the ONB subsystem.

implementation is usually based on patented hardware solutions; in this study a Field Programmable Gate Array-based voter is used, in particular a couple of FPGAs has been used in order to improve reliability. The Power Supply of EVC is the most critical unit of ONB from a reliability point of view, hence the reference architecture includes two redundant Power Supply units. The backplane of EVC consists of a redundant system bus. EVC is connected to several I/O peripherals. The communication with the trackside is provided by the RTM unit, which exchanges information through the GSM-R network. Other I/O units are: the BTM unit, which reads data from balises; the TIU unit, that is the interface to the train brakes and engine; the Odometer (ODO) unit, used to evaluate train speed and position, and the MMI unit, that is the interface to the train driver.

2.3. *The TCS*

While the lineside subsystem is distributed on the track, TCS in concentrated in a few points and mainly consists of four components also listed in Table 1. The most important of them is the Radio Block Centre (RBC) which is a computing system whose aim is to control the movements of the set of trains on the track area that is under its supervision, in order to guarantee a safe inter-train distance. In this work, we do not address the issues related to the RBC–RBC communication and the RBC hand-over.

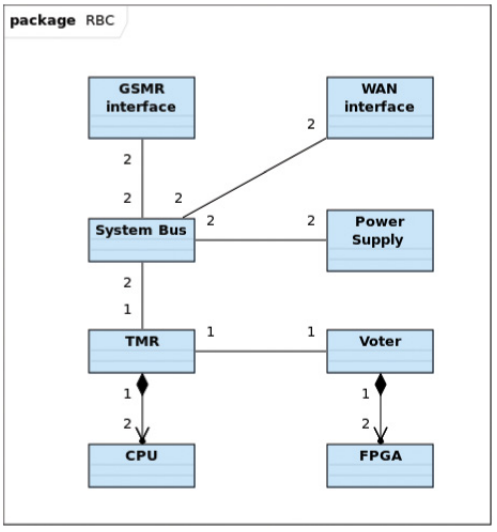

Fig. 3. Class diagram of the RBC component.

[a]The voter is accepted as a single point of failure in this reference architecture, hence its reliability is a critical factor.

The RBC computing system is the core component of the Level 2 trackside infrastructure. The class diagram in Fig. 3 shows the RBC architecture in more details. It is similar to the architecture of the EVC. The backplane consists of redundant system bus. The main difference between RBC and EVC is in the communication subsystems: a WAN interface is used to communicate with other RBCs, and GSM-R interfaces are used to communicate with trains. RBC is responsible for controlling all the trains in its supervised area, hence its availability is critical. For this reason *RBC has to be continuously supervised by at least one technician* and it is supposed to be easily maintained "on-line". Proper repairing policies have to be planned and applied whenever a fault is detected (see also Ref. 29), *Vice versa, the ONB subsystem — EVC included — cannot be repaired "on−the−fly" if a failure occurs* to one of its components. *This difference will be taken into account by adopting different modeling techniques for ONB and RBC*, as described in Sec. 4.[b]

2.4. *The movement authority*

The whole railway track managed by an ERTMS/ETCS-based system is usually divided into several sub-tracks, each of which is supervised by a single RBC. The RBC computing system is in charge of controlling a number of trains in order to guarantee their headway, which depends on performance and safety requirements trade-offs. Messages between EVC and RBC are transmitted via GSM-R using the EuroRadio protocol which also provides channel monitoring by means of distributed time-stamping and watchdog timers. In particular, the main objective of the train control system is to timely transmit to each EVC its up-to-date Movement Authority (MA) and the related speed profiles. The MA contains information about the distance a train may safely cover, depending on the status of the forward track. At ERTMS Level 2, the MA is calculated and transmitted to the trains by the RBC. Each ONB subsystem periodically sends via GSM-R a Position Report (containing the train position and speed) to RBC.[c] The MA message is also used in some implementations as a channel monitoring message. If a train does not receive a new MA within a fixed number of seconds after the last received message, EVC tries to re-establish the connection within a specified timeout period and the following situations may happen:

— EVC receives a new MA from the trackside within the specified deadline: in this case normal conditions are restored and it keeps moving according to this updated MA (Full Supervision operating mode);
— EVC receives at least one valid message (not a MA message) from the trackside within the specified deadline: in this case it has to stop according to the

[b]TCS is not limited to RBC; other components are not included in our analysis because they are outside of the boundary of the ERTMS/ETCS specification.
[c]Each RBC has to communicate with its neighboring RBCs in order to manage the passage of a train from one sub-track to the next, executing the so-called hand-over procedure.

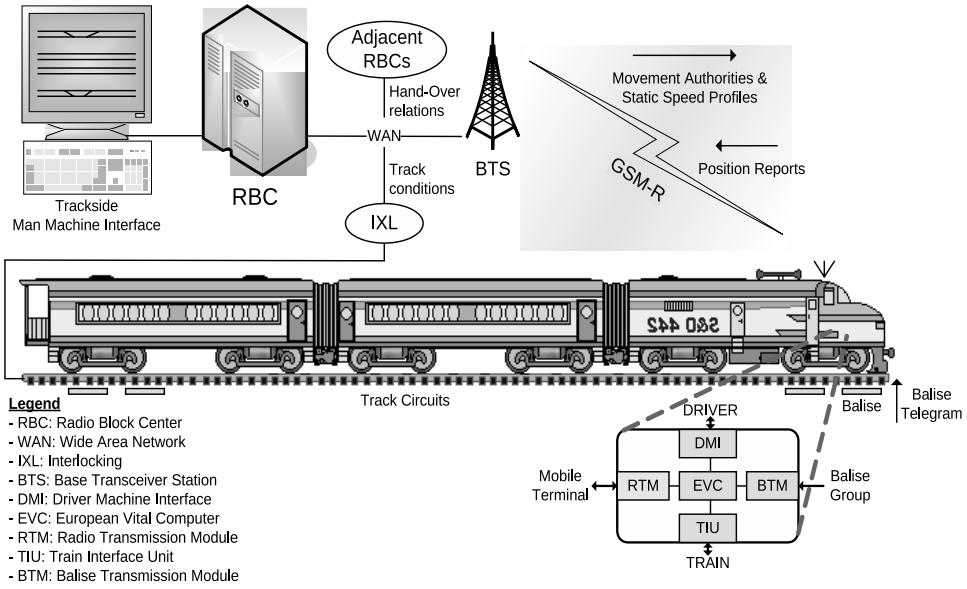

Fig. 4. ERTMS/ETCS system.

information contained in the last valid MA, while braking the train is still in Full Supervision operating mode;

— EVC does not receive any correct message within the specified deadline: in this case the train will start the braking procedure immediately. After braking, the train may start to move under the control of the driver (Staff Responsible operating mode).

The last scenario may lead to the failure of the supervision system, as explained in Sec. 3. Figure 4 gives an overall view of ERTMS/ETCS Level 2.

3. Requirements and Measures

In this section, we describe ERTMS/ETCS failure modes and the related quantitative requirements. The standard defines the following failure modes of the system, listed in decreasing order of severity:

— immobilizing failures,
— service failures,
— minor failures.

They correspond to different levels of performance degradation of the system: an IF occurs when at least two trains on the track are no more under the RBC supervision. This situation occurs, for example, if MAs cannot be issued. In this case, the trains will brake, and will be able to re-start only by switching to a Staff Responsible operating mode. A SF occurs when at most one train on the track is no more under

the RBC supervision. A *Minor Failure* is a failure that cannot be classified neither as IF nor as SF. In this paper, we focus on IFs and SFs.

Two different approaches — both allowed by the ERTMS/ETCS specifications — can be followed to demonstrate compliance with RAM requirements:

(1) "Constituent level": the requirements are specified on — and they must be met by — each subsystem and/or component. This is a very conservative approach, since it explicitly takes into account the Mean Time Between Failures (MTBF) values of the single modules. Such an approach implies more restrictive design choices and it may cause nonbalanced allocation of costs among components.
(2) "System level": the requirements are specified on system failure modes.

The second approach is potentially more effective, however it is rather difficult to pursue because of the required modeling effort. The work presented in this paper contributes to the definition of a "system level" approach, which (to the best of our knowledge) is currently not adopted by any ERTMS/ETCS supplier. Furthermore, such an approach allows investigating about the coherence of constituent level requirements.

Our study addresses the following reliability indices:

— system availability, with respect to hardware failures and transmission errors (A_O);
— system unavailability with respect to IF, due to hardware failures and transmission errors (U_{IF});
— system unavailability with respect to SF, due to hardware failures and transmission errors (U_{SF});
— system unavailability due to transmission errors (U_{TX});
— MTBF of ONB with respect to IF ($\mathrm{MTBF}_{\mathrm{IF}}^{\mathrm{ONB}}$);
— MTBF of ONB with respect to SF ($\mathrm{MTBF}_{\mathrm{SF}}^{\mathrm{ONB}}$);
— RBC unavailability (U_{RBC}).

The RAM requirements related to these indices are summarized in Table 2.

The analyses are performed by integrating the following submodels:

— RBC hardware failure model,

Table 2. Reliability requirements.

Reliability indexes	Requirements
A_O	> 0.99984
U_{IF}	$< 1.6 * 10^{-5}$
U_{SF}	$< 1.44 * 10^{-4}$
$\mathrm{MTBF}_{\mathrm{IF}}^{\mathrm{ONB}}$	$> 2.7 * 10^{6}$ [h]
$\mathrm{MTBF}_{\mathrm{SF}}^{\mathrm{ONB}}$	$> 3 * 10^{5}$ [h]
U_{RBC}	$< 10^{-6}$
U_{TX}	$< 1.6 * 10^{-5}$

— ONB hardware failure model,
— RBC timing failure model.

Dealing with safety-critical systems, we can reasonably neglect the effects of systematic software faults on system availability due to high testing and verification activities required for the software. Another important hypothesis must is that we deal with constant failure rates for components. The introduced RAM requirements are related to the operational phase of the system which starts after an initial testing period (also motivated by the safety critical nature of the application). Thus we can neglect the contribution related to the "infancy mortality" of the well-known bathtub curve. Moreover preventive maintenance policies and limited mission times allow us to neglect the "wear out" contribution of the bathtub curve, too. Constant failure rates can be used in this case to assess availability/reliability at the system level.

For the evaluation of the ONB failure rate, we can simply adopt FT, one of the most widespread, easy to use and efficient formalism for reliability modeling. In our analysis we consider some COTS components and other custom modules which are not commercially available. For the RBC, it is important to account for the maintenance policy, hence the RFT formalism is adopted.[26] In order to evaluate the third contribution, the behavior of the interaction between RBC and ONB is modeled by means of GSPN. GSPNs have been shown in several works to be a suitable formalism for modeling both performance and reliability of heterogeneous computer systems.[30] By using a GSPN model we are able to evaluate, for instance, the impact of GSM-R availability on system performance. Finally, the three contributions described above are integrated in a BN model representing the overall availability of the system with respect to both IFs and SFs. Section 4 provides a detailed description of reliability measures and model parameters.

4. Availability Modeling

As aforesaid, such an approach allows modelers to cope with the complexity of systems and promotes reuse of sub-models.

4.1. *Bayesian model of the overall system*

In this section, we describe the system level failure model, which is built using the BN formalism.
IFs can be caused by the following events:

— a hardware failure in at least two ONBs,
— a hardware failure in at least one RBC,
— a delay in the MA delivering to at least two ONBs.

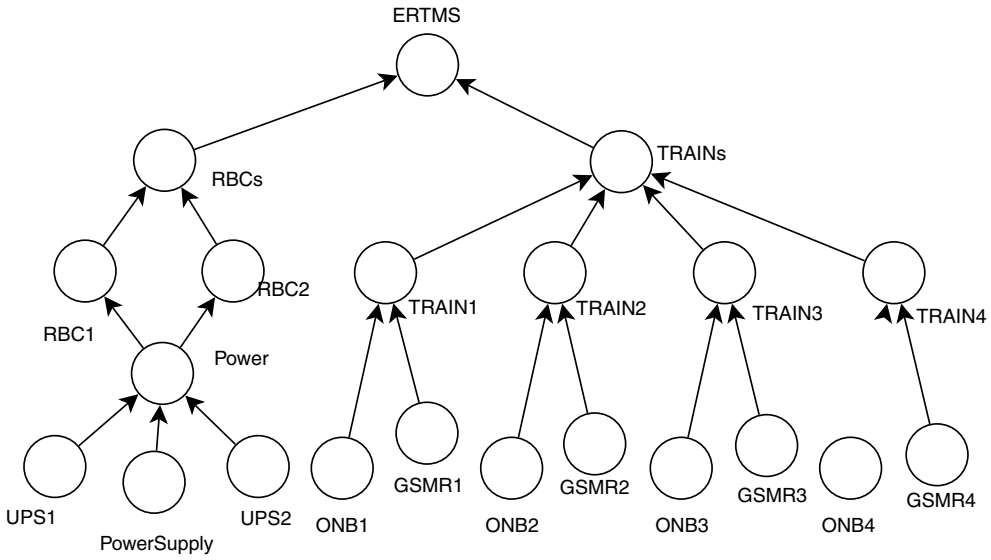

Fig. 5. Contributions of the different sub-models to the overall analysis.

SFs can be caused by the following events:

— a hardware failure in one ONB,
— a delay in the MA delivering to at most one ONB.

These considerations are a consequence of realistic system configurations, in which at least two trains are under the supervision of a single RBC. Therefore, a single RBC unavailability affects the possibility to control at least two trains, thus causing an IF. The use of BN allows engineers to easily model common modes of failure, such as the loss of power in the central control room where the RBCs are located. The second reason for the choice of BN is the possibility to use a single model for both IFs and SFs by using tri-state events. The model, depicted in Fig. 5, is hierarchically structured: top event models the ERTMS system failure and two main branches model the on-board and trackside contributions, respectively. The ERTMS event is a discrete stochastic variable whose possible values are: IMMOBILISING, SERVICE and NONE. The Conditional Probability Table (CPT) of this event is reported in Table 3. The CPT models rules which relate subsystems failures to system ones listed at the beginning of Sec. 3.[d]

In the network, three classes of events can be identified which need further analysis by developing the models mentioned before: RBC events (RBC1 and RBC2),

[d]MINOR failures are not considered in this study, therefore the results obtained for the NONE state actually refer to a "minor or no failure" state.

Table 3. ERTMS conditional probability table.

RBCs	TRAINs	IMMOBILISING	SERVICE	NONE
OK	AllUp	0	0	1
OK	OneKO	0	1	0
OK	TwoKO	1	0	0
OK	ThreeKO	1	0	0
OK	AllKO	1	0	0
KO	AllUp	1	0	0
KO	OneKO	1	0	0
KO	TwoKO	1	0	0
KO	ThreeKO	1	0	0
KO	AllKO	1	0	0

GSM-R events (GSMR1 to GSMR4) and ONB events (ONB1 to ONB4). Each of these events is associated with a subsystem model. In particular:

— ONB: a FT model of the ONB subsystem is needed in order to obtain ONB unavailability due to hardware failures (under the "nonrepairable" hypothesis) (see Sec. 4.2);
— RBC: a RFT model of RBC is needed in order to take into account realistic (nontrivial) repair policies (see Sec. 4.3);
— GSM-R: a GSPN model is needed to analyze the performance of the RBC in the MA assignment and delivery procedure (see Sec. 4.4).

4.2. *FT model of the ONB*

Failure rates are traditionally evaluated using FT models. However, they do not allow modelers to take into account complex repair strategies and modeling common mode of failures is not natural as in other formalisms. As ONB is assumed to be not repairable on-line (there is no on-board technician), a FT can represent the ONB failure model. Given the architecture of the subsystem in Fig. 2, the FT can be built by a straightforward inspection of the class diagram. The FT model of the ONB is shown in Fig. 6. All the components of the subsystem are at least double redundant, thus the fault of a single replica does not directly imply a subsystem failure. The computing subsystem is assumed to be based on the Triple Modular Redundant (TMR) architecture: a CPU failure event only happens if more than one CPU is faulty, because two of them can still support the safe operation of the EVC in a "two out of three" configuration.

4.3. *RFT model of RBC*

The RBC structure is shown in the class diagram in Fig. 3. The RBC hardware failures have been modeled using the RFT formalism in order to account for articulated on-line maintenance policies. In particular, RFTs allow to model and analyze[26]:

— which fault condition will start a repair action;

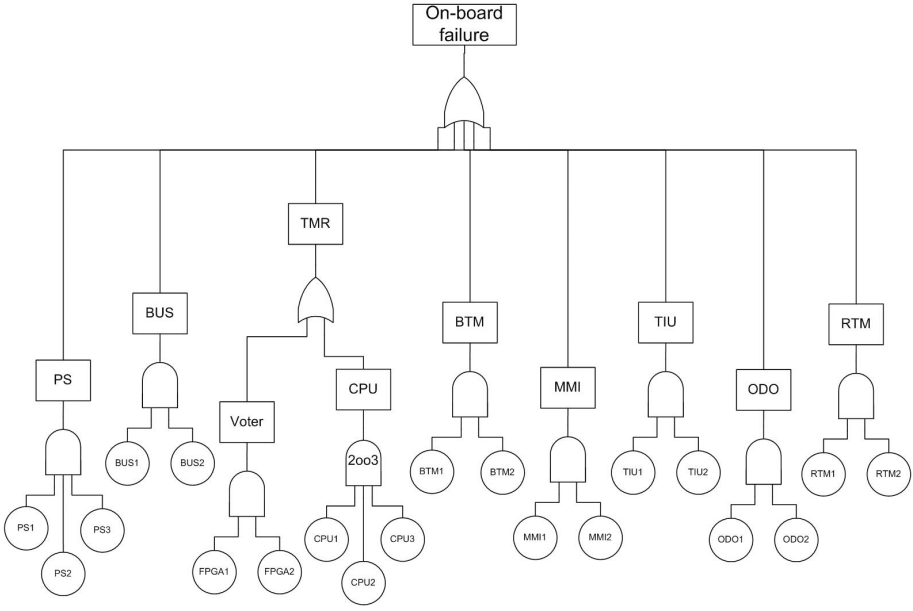

Fig. 6. The FT model for the ONB.

— the repair policy, including the repair algorithm, the repair timing and priority, and the number of repair facilities;
— the components in the system which are actually repairable.

A RFT model is a simple FT with the addition of a new language element called Repair Box (RB). The basic FT is obtained as usual, then RBs are added in order to model repair actions. Each RB is associated with a repair policy and connected by two arcs: the first links the RB to the event which triggers the repair action; the second connects the RB to the Basic Events (BE) (i.e., the tree leaves) on which it operates (i.e., the repairable components). The trigger event can also be expressed by a boolean combination of fault events: in this case, a boolean function is represented in the RFT by a box labeled "$f(x)$" connected between the triggering events and the RB. Therefore, the RFT model of the subsystem can be obtained in two steps: in the first, the FT of the subsystem is built by inspection of its class diagram; in the second, the repair policies are included in the model by defining which conditions will trigger the repair policies and on which sub-tree (i.e., subset of components) each of them will be applied. As shown in Fig. 7, several repair policies have been applied to the RBC (the RBs are represented by triangles):

— a RB triggered by a RBC system failure,
— a RB for each component, triggered by a fault in its components.

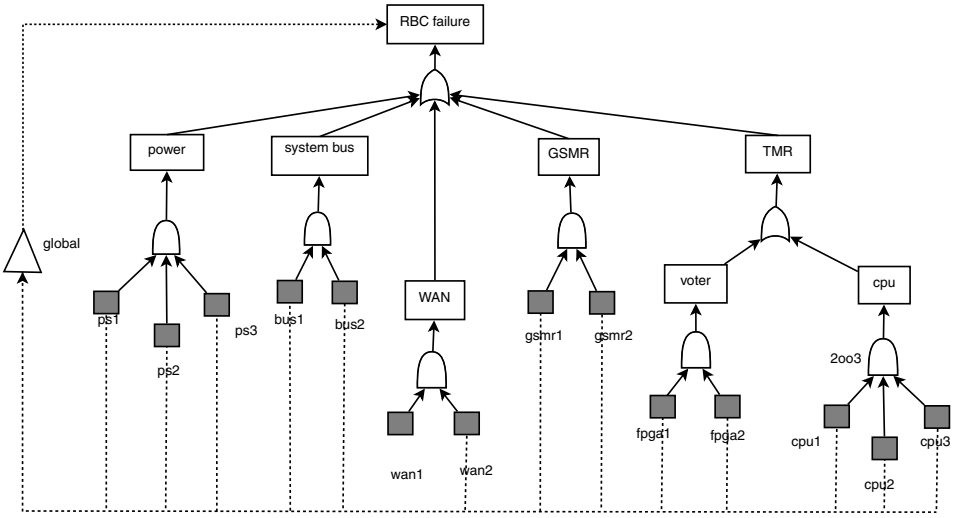

Fig. 7. RFT model of the RBC.

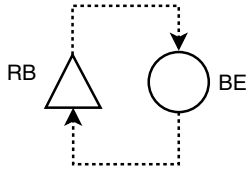

Fig. 8. Repairable component in RFT model.

In Fig. 7, a graphical artifice has been used to improve picture readability: a gray square stands for BE and its associated RB as depicted in Fig. 8. All RBs share the same repair resources, that is the technicians in charge of performing the repairs. Two levels of repair actions are implemented: the first level, composed of all the RBs of the single subsystems, represents preventive maintenances since repair actions are triggered before a RBC failure; the second level only contains the RB related to a RBC failure, representing an emergency maintenance intervention. The first level RBs works in parallel, and compete for resources with a selectable policy (see Ref. 29); each of them complete its repair action in an exponentially distributed time depending on the components it is applied to. Although preventive, this kind of repair action is only on-demand, because it is always triggered by a component fault. The second level RB has a higher priority with respect to the first: when it is activated, it stops any other repair action and gains the control of all repair resources.

The introduction of RBs requires the RFT to be solved by state space calculation and in particular by means of a translation into an equivalent GSPN[26]: this

technique may be computationally very expensive, so it must be applied only to those subtrees that actually require it, namely those subtrees whose event nodes state depend on the action of some RBs. In the proposed RFT model the minimum subtree that must be solved in such way is equal to the whole tree so the entire tree must be transformed into a GSPN.

We will consider three key parameters related to the Mean Time To Repair of the faulty units: (1) $\mathrm{MTTR_{SYS}}$, which indicates the MTTR of the entire RBC (including the time to restart); (2) $\mathrm{MTTR_{CARD}}$, which is the MTTR for line replaceable components (e.g., WAN interface); (3) $\mathrm{MTTR_{BUS}}$, associated with components which are harder to be replaced (e.g., due to their physical accessibility).

4.4. *GSPN model of MA delay*

The GSPN formalism has been chosen to model the MA delivery procedure. GSPNs are widely used for performability modeling due to their ability to cope both with deterministic and stochastic timed events.[10,31,32] In Sec. 1, we reported some former works on the analysis of performability models of ERTMS/ETCS. They focus on the GSM-R network reliability rather than on the timeliness of the computation, which is taken into account in this study. The model is depicted in Fig. 9 and can be easily divided into three main submodels (from right to left): the RBC side, the GSM-R channel and the ONB side.

The first submodel represents the RBC communication process (see Fig. 10). In the network, two places (CONN_UP and CONN_DOWN) model the availability of the GSM-R connection: only when the connection is up (CONN_UP), the RBC can send channel monitoring messages to the ONB: this fact is modeled by means of an inhibitor arc from CONN_DOWN to RBC_RX. The two transitions, which model the state change of the GSM-R connection, are ruled by a death–birth Markovian process with λ and μ such that the global availability of GSM-R network is within the RAMS specification of 0.9995. When the GSM-R connection is up, the RBC can send messages to the ONB by means of the RBC_RX transition that is a deterministic timed transition (due to the fact that messages are sent periodically). The delivery of messages keeps alive the connection between the two ends, allowing for the supervision of train movement.

The second submodel (see Fig. 11) is specifically related to the performance of the GSM-R network. The messages, sent by RBC, are stored in GSMR_BUFFER place and delivered after a stochastic delay, which is assumed to be exponentially distributed with a rate of T_COMM. Upon message reception (in place TX_BUF), the ONB verifies data integrity. If the message is corrupted, an event that occurs with a probability of P_ERR, the TX_FAIL transition fires, otherwise the TX_OK fires: in this case, a retransmission request is notified to the RBC by means of RE_TX, R_INJECT network elements. In the model an inhibitor arc is also present from GSMR_BUFFER to RBC_RX transition; it models that the RBC does not add a new message in the buffer until the older one has been sent to the ONB.

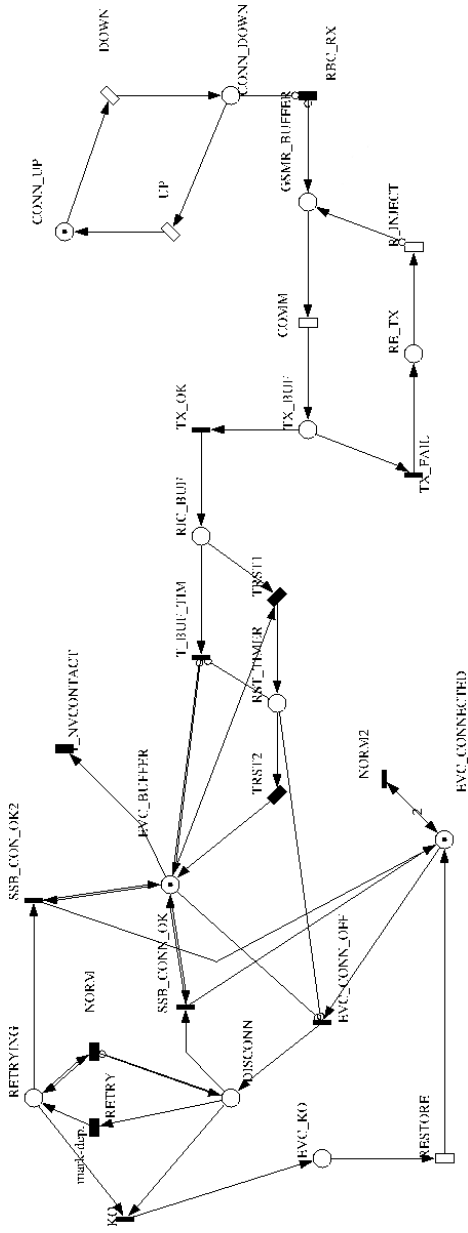

Fig. 9. The structure of the GSPN performability model.

Upon reception of each new message, the EVC starts the timer for the management of channel monitoring: this is modeled by the network depicted in Fig. 12. Messages are stored in RIC_BUFFER place, which in turn feeds the EVC_BUFFER place; this can be done in two different ways: if no validity timer has been set

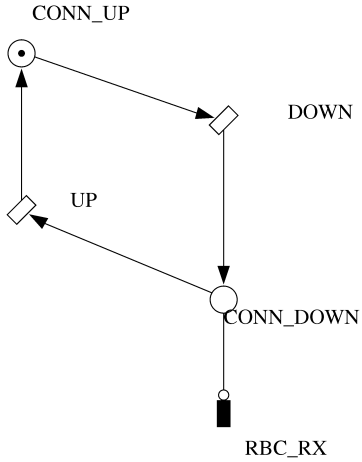

Fig. 10. RBC communication module in vital communication model.

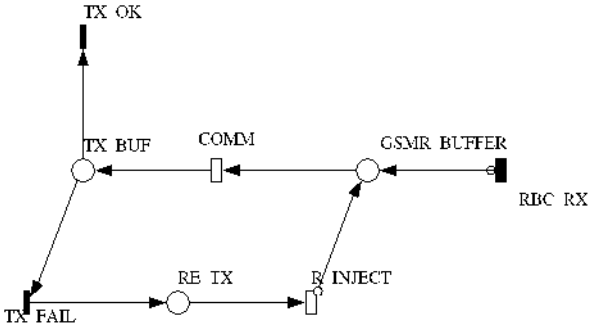

Fig. 11. GSM-R module in vital communication model.

(condition modeled by the presence of a token in EVC_BUFFER place), tokens flow through T_BUF_TIM transition, otherwise the sequence of transitions TRST1 and TRST2 can fire allowing the reset of such timer. Tokens are drained from EVC_BUFFER by the T_NVCONTACT timed transition (with deterministic rate 1/TNV), the firing of which represents the message timeout. After TNV seconds, a loss of supervision is detected and the train starts braking. In order to improve resiliency with respect to "radio holes", ERTMS/ETCS is capable of resuming a lost connection by performing NUM_RETRY attempts, one each T_RETRY seconds. If a new message is received during these attempts, the connection is restored and the system returns to a full supervision operating mode. After NUM_RETRY unsuccessful attempts, the train must be operated using degraded operating modes and a new connection request can be issued only upon reception of a new balise message, after an average time of T_RESTORE seconds.

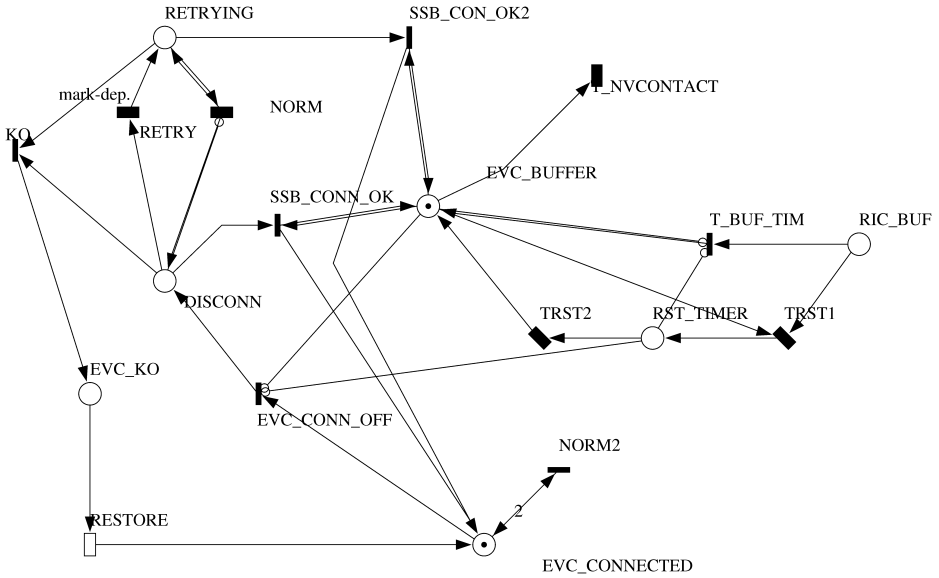

Fig. 12. On-board timing module in vital communication model.

5. Results

In this section, we present the results of our study whose main goal is to find a set of parameters capable of satisfying the overall reliability of the system as requested by the ERTMS/ETCS standard. A sensitivity analysis has been performed for each submodel in order to identify the most critical components and the boundary values for their parameters. Due to the nature of our study, the cost impact of components is only considered in a qualitative way. Tables 4 and 5 show the nominal values of parameters involved in the analyses. These parameters are split into two tables: one groups COTS components, the other ERTMS custom components.

5.1. *ONB unavailability contribute evaluation*

The ONB model evaluation is performed by using the values listed in Tables 4 and 5. The results obtained with these values for the ONB and for each of its subsystems are reported in Table 6.

Table 4. COTS reliability metrics.

Unit	MTBF [h]	MTTR [h]
CPU card	$1.35 * 10^5$	0.0833
Bus	$2.25 * 10^5$	0.25
FPGA	$3.33 * 10^8$	0.25
Power Supply	$5.5 * 10^4$	0.0833
GSM-R interface	$1.752 * 10^5$	0.0833
WAN interface	$4 * 10^5$	0.0833

Table 5. ERTMS unit reliability metrics.

Unit	MTBF [h]
RTM	10^6
BTM	10^8
Odometer	10^7
MMI	10^7
TIU	10^7

Table 6. Summary of the evaluated MTBF of the ONB and its subsystems.

Subsystem	MTBF [h]
BTM	$1.5 * 10^8$
RTM	$1.5 * 10^6$
MMI	$1.5 * 10^7$
TIU	$1.5 * 10^7$
Odometer	$1.5 * 10^7$
TMR	$1.125 * 10^5$
Voter	$4.95 * 10^8$
Bus	$3.375 * 10^5$
Power	$8.25 * 10^4$
ONB	$6.4576 * 10^4$

Table 7. Sensitivity analysis of the ONB MTBF [10^4h].

	$0.1x$	$0.5x$	$1x$	$5x$	$10x$
RTM	5.5458	6.4064	6.4576	6.4761	6.4768
BTM	6.4574	6.4576	6.4576	6.4576	6.4576
Odometer	6.4386	6.4569	6.4576	6.4578	6.4578
MMI	6.4386	6.4569	6.4576	6.4578	6.4578
TIU	6.4386	6.4569	6.4576	6.4578	6.4578

It is noticeable from these preliminary results that the power supply subsystem is a bottleneck of the system and that, as expected, all COTS have a major impact, while the voter does not limit the computing subsystem. Table 7 summarizes the quantitative results of sensitivity analysis performed on the FT model described in Sec. 4.2. Each cell of the table contains the value of the ONB MTBF, computed keeping all the values of the MTBFs of COTS components at their nominal values, all the ERTMS unit MTBFs at their nominal values except the one indicated at the start of the row: for such components the nominal value of MTBF is multiplied by the factor indicated at the top of the column.

Therefore, a good trade-off for free parameters can be obtained with $\mathrm{MTBF_{BTM}} = \mathrm{MTBF_{RTM}} = \mathrm{MTBF_{MMI}} = \mathrm{MTBF_{TIU}} = \mathrm{MTBF_{Odometer}} = 10^7$,

that gives an MTBF for the ONB of $6.4766 * 10^4$.[e] Further redundancy can be used for the components for which it is more difficult (or expensive) to obtain high MTBF. For instance, we found out that the further replication of the less reliable RTM with a third replica configured as a hot spare leads, in the same conditions of the previous analysis, to an overall MTBF of $6.4752 * 10^4$ for the ONB, which is very similar to the previous result. In order to evaluate the system level impact a simple conversion is needed, by using the formula $U = \frac{\text{MTTR}}{\text{MTBF+MTTR}}$. As required in Ref. 15, we assume that MTTR of the ONB is 1.737 h. This takes to an overall ONB unavailability of $2.682 * 10^{-5}$. According to Table 2, the MTBF of the ONB $6.4752 * 10^4$ does not satisfy the reliability requirement stated for this subsystem according to the "constituent level" approach. Nevertheless at the end of this section we will show how system requirements can be fulfilled at a global level according to our hypothesis of global optimization made in Sec. 3.

5.2. *RBC unavailability contribute evaluation*

MTBF values of COTS components of the RBC are given in Table 4, while reference values for the repair parameters are given in Table 8. These values are average times needed to perform the on-line repair of a given component: components are grouped in three classes since the repair action is assumed to be a component replacement action, hence the repair time is dependent on component accessibility and not on its nature.

Assuming the value of the parameters listed in Table 8 and the standard repair policy described in Sec. 4.3, the evaluated RBC unavailability is $3.394 * 10^{-6}$: this value has been found analyzing the RFT in the Sec. 4.3 by means of steady-state analysis. At first, in order to evaluate the effects of MTTR_{SYS} on RBC unavailability, its value has been varied according to a sensitivity analysis as for ONB analysis in Sec. 5.1, within an interval of values centered on the reference value; the same analysis has been performed for $\text{MTTR}_{\text{CARD}}$ and MTTR_{BUS}. In Table 9 we report the results of the analysis.

Effects of variations in MTTR_{SYS} are more evident than in the other two, since this parameter represents the emergency repair following a system failure. Reducing

Table 8. Reference parameters for repair.

Repair parameter	Description	MTTR [min]
MTTR_{SYS}	Mean time for overall system repair action	30
MTTR_{BUS}	Mean time for Bus and FPGA component repair actions	15
$\text{MTTR}_{\text{CARD}}$	Mean time for all other component repair actions	10
N_{RES}	Number of repair resources	1

[e]This result is not present in Table 7 because this case refers to the contemporaneous variation of two parameters from the values in Table 6.

Table 9. RBC unavailability with respect to repair times.

	0.5x	1x	2x
$MTTR_{SYS}$	$1.697 * 10^{-6}$	$3.394 * 10^{-6}$	$6.79 * 10^{-6}$
$MTTR_{BUS}$	$3.263 * 10^{-6}$	$3.394 * 10^{-6}$	$3.66 * 10^{-6}$
$MTTR_{CARD}$	$2.85 * 10^{-6}$	$3.394 * 10^{-6}$	$4.485 * 10^{-6}$

$MTTR_{SYS}$ corresponds to reducing recovery times, which is usually not straightforward. The results also show that the variation of the other parameters has a limited impact on RBC unavailability. By adding a further repair resource and leaving all the other repair parameters to their reference values, the RBC unavailability decreases to $1.37 * 10^{-6}$, slightly improving the former result. On the contrary, the assignment of one resource to more than one RBC dramatically worsens RBC unavailability to $7.11 * 10^{-5}$. It is possible to introduce the concept of priority among the repair actions. The best strategy for the priority assignment consists in assigning the highest repair priority to the less redundant subsystems: in this case the RBC unavailability is $3.265 * 10^{-6}$. The combination of all the factors improving the RBC unavailability (higher priority to less redundant components, two repair facilities, $MTTR_{SYS} = 15$ min) leads to an overall unavailability for the RBC of $6.736 * 10^{-7}$. Results are graphically reported and compared in Fig. 13 (further details are in Ref. 29).

5.3. *RBC-EVC performance contribute evaluation*

The GSPN has been studied using a set of reference values for model parameters which have been defined on the basis of ERTMS/ETCS requirements (see Table 10).

In the following, we report a description of these parameters:

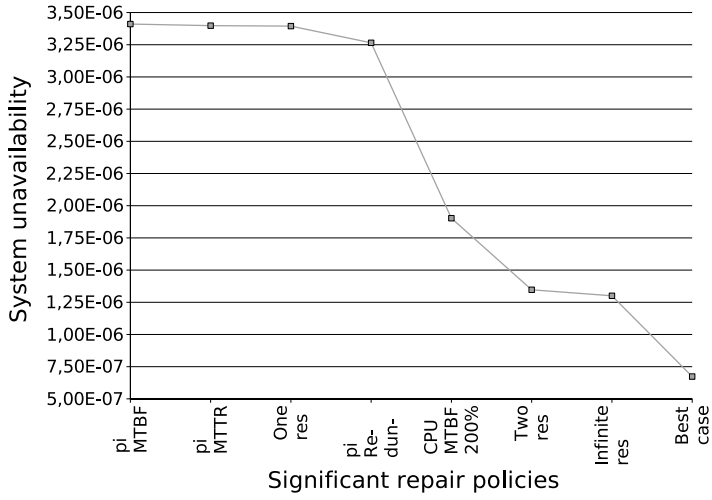

Fig. 13. RBC overall analysis results.

— NUM_RETRY: number of reconnection attempts by the ONB;
— T_RESTORE: mean time (in seconds) from a disconnection to the next balise group commanding a recall to the RBC;
— T_RETRY: time (in seconds) between reconnection attempts;
— TNV: time-out (in seconds) after that a received message is no more valid;
— T_MESS: time (in seconds) between monitoring messages sent by RBC;
— CONN_UNAVAIL: unavailability of GSM-R connection;
— T_COMM: mean message transmission time (in milliseconds) on the GSM-R network;
— P_ERR: probability of a messages being corrupted during transmission.

Several simulations have been performed in order to evaluate system unavailability caused by transmission and timing errors, represented in the GSPN by the mean number of tokens EVC_KO place. Simulation is needed because there are several markings where more than one transition with nonexponentially distributed firing delay is enabled.[33] The results have been computed with a confidence level of 95% and a relative error of 1%. The unavailability due to transmission and timing errors of $5.9 * 10^{-4}$ is far from fulfilling the ERTMS requirement on U_{TX} stated in Table 2. A sensitivity analysis has been conducted in order to identify availability bottlenecks in the model. The results of the analysis are summarized in Table 11. Note that no analysis has been performed for the NUM_RETRY parameter since its value is fixed by the standard.

Parameters T_RETRY, T_RESTORE and CONN_UNAVAIL are the ones that mainly contribute to RBC unavailability. System behavior analysis brings us to state that the optimal value of some parameters (like TNV) is the result of a trade-off between reliability and safety requirements. Therefore, it is more useful to focus the analysis on the variations of CONN_UNAVAIL and T_RESTORE, since they can be easily varied without affecting system safety.

5.4. *Global model analysis*

As already mentioned, all the developed sub-models have been integrated in the global BN model depicted in Fig. 5. The model represents ERTMS system

Table 10. Communication GSPN model parameters.

Parameters	Value
NUM_RETRY	3
T_RESTORE	600
T_RETRY	30
TNV	8
T_COMM	500
P_ERR	10^{-7}
CONN_UNAVAIL	$5 * 10^{-4}$
T_MESS	4

unavailability with respect of IFs and SFs. First of all, a marginal distribution of the ERTMS event is calculated; this metric shows the distribution probability of system unavailability with respect of its values: IMMOBILISING, SERVICE and NONE. This first analysis has been conducted according to Table 12 that shows the parameter assignment in the events that represent unavailability in components and subsystems: for UPS and PowerSupply components, commercial values from data sheets were chosen; for the other subsystems, the values have been selected from the previous sub-model initial analyses.

The results of this analysis are reported in Table 13 and they highlight a situation in which, according to Table 2, the requirement on IFs ($U_{\mathrm{IF}} < 1.6 * 10^{-5}$) is met but the other on SFs ($U_{\mathrm{SF}} < 1.44 * 10^{-4}$) is not.

Table 11. GSPN sensitivity analysis.

Name	Variation	Result
Less time for retry	$T\_RETRY = 20$	$6.9 * 10^{-4}$
More time for retry	$T\_RETRY = 40$	$5 * 10^{-4}$
More time to restore	$T\_RESTORE = 350$	$6.6 * 10^{-4}$
Less time to restore	$T\_RESTORE = 250$	$5.1 * 10^{-4}$
Smaller message time-out	$TNV = 7$	$6.1 * 10^{-4}$
Greater message time-out	$TNV = 9$	$5.8 * 10^{-4}$
Greater communication delay	$T\_COMM = 600$	$5.9 * 10^{-4}$
Smaller communication delay	$T\_COMM = 400$	$5.8 * 10^{-4}$
Shorter messages time interval	$T\_MESS = 3$	$5.9 * 10^{-4}$
Longer messages time interval	$T\_MESS = 5$	$5.7 * 10^{-4}$
Higher probability of message corruption	$P\_ERR = 5 * 10^{-7}$	$5.9 * 10^{-4}$
Lower probability of message corruption	$P\_ERR = 5 * 10^{-8}$	$5.8 * 10^{-4}$
Lower availability of GSM-R connection	$CONN\_UNAVAIL = 10^{-3}$	$9.9 * 10^{-4}$
Higher availability of GSM-R connection	$CONN\_UNAVAIL = 10^{-4}$	$1.1 * 10^{-4}$

Table 12. Parameters of BN system model.

Parameter	Value
Power supply	$1.54 * 10^{-5}$
UPS	$1.25 * 10^{-6}$
RBC	$5 * 10^{-6}$
GSM-R	$5.9 * 10^{-4}$
ONB	$2.68 * 10^{-5}$

Table 13. Marginal distribution of ERTMS event.

System failure	Value
IMMOBILISING	$1.228 * 10^{-5}$
SERVICE	$2.46 * 10^{-3}$
NONE	0.99752

Table 14. Sensitivity analysis GSM-R versus ERTMS.

GSM-R unavailability	System SF probability
$5.9 * 10^{-4}$	$2.46. * 10^{-3}$
10^{-4}	$5.06 * 10^{-4}$
$5 * 10^{-5}$	$3.07 * 10^{-4}$
10^{-5}	$1.47 * 10^{-4}$
$5 * 10^{-6}$	$1.27 * 10^{-4}$

In order to solve this requirement mismatch and to find the availability bottlenecks of the system, another kind of analysis has been conducted. By means of marginal expectation on the different components and subsystems events, it was possible to state that GSM-R events are bottlenecks. Then a sensitivity analysis has been pursued on the model varying only the probability of these events in order to evaluate which of the GSM-R network unavailability values satisfies the system requirement on SF. The result of this analysis has been reported in Table 14. All the analyses have been performed by means of JavaBayes.[34]

A set of GSM-R network parameters such that GSM-R unavailability lies between 10^{-5} and $5 * 10^{-6}$ must be searched. In order to pursue this analysis, we focus our attention on the most sensitive GSM-R network parameter that is the unavailability of the mobile connection. Further analyses found that for values of CONN_UNAVAIL lesser or equal to $2.5 * 10^{-5}$ both the requirements on the IFs and SFs at a global level can be fulfilled. This value is fully compatible with the hypothesis of double and independent radio coverage, on which several existing Italian high speed lines projects are based. The details of such analyses have not been extensively reported for the sake of brevity.

6. Conclusion

ERTMS/ETCS is a distributed heterogeneous critical system, with strict and hard dependability requirements. In this paper, we studied ERTMS/ETCS using a modeling approach that suits for complex computer-based critical systems requiring dependability evaluation since the early stages of their development cycle. We went through a preliminary phase, in which we decomposed the system into smaller parts to better understand and model the system structure and behavior, and subsequent modeling/evaluation phases. Based on the utilization of formal modeling techniques, the modeling phase was performed on both the models representing the sub-systems and on a global model of the system.

The paper demonstrates the ability to fulfil ERTMS/ETCS RAM requirements by a reference architecture finding a good trade-off between the costs of the single components (inverse proportional to their reliability levels) and the matching of the global availability requirements. According to the two design methods described in Sec. 3, this paper shows how to pursue a system level approach by means of modularity. It allows the designer to find the best mix of parameters that both fulfil

specification requirements and optimize components cost: in fact the designer who follows the component level approach is destined, against a simpler design process, to fulfil requirements with more expensive components (i.e., components with higher MTBFs). The proposed approach is supported by the use of a multiformalism and multisolution integrated framework as OsMoSys that allows the integration of both different formalisms and different solvers by means of model driven approaches.[20,35] The work presented in this paper is going to be extended to model other meaningful aspects of the system, including a deeper model and analysis of the GSM-R network that has been proved to be the reliability bottleneck of the system.

This work has been conducted with only freely available material: no reserved data nor reserved specification has been used. ERTMS/ETCS reference architecture has been determined by means of public ERTMS specification and COTS component reliability data have been extracted from commercial data sheet analysis available on the Internet.

References

1. UIC, ERTMS/ETCS class1 system requirements specification, ref. SUBSET-026, issue 2.2.2 (2002).
2. M. W. Pollack, Train control. Automating the world's railways for safety, *IEEE Potentials* **17**(1) (1998) 8–12.
3. A. U. H. Sheikh, D. C. Coll, R. G. Ayers and J. H. Bailey, ATCS: Advanced train control system radio data link design considerations, *IEEE Trans. Veh. Technol.* **39**(3) (1990) 256–262.
4. A. Amendola, L. Impagliazzo, P. Marmo and F. Poli, Experimental evaluation of computer-based railway control systems, *Proc. 27th Int. Symp. Fault-Tolerant Computing* (IEEE Computer Society, 1997), pp. 380–384.
5. N. Aoumeur and G. Saake, Towards an adequate framework for specifying and validating runtime evolving complex discrete-event systems, in *Proc. Workshop on Modelling of Objects, Components and Agents* (*MOCA 2001*) (2001), pp. 1–19.
6. J. Padberg, L. Jansen, H. Ehrig, E. Schnieder and R. Heckel, Cooperability in train control systems: Specification of scenarios using open nets, *J. Integr. Des. Process Sci.* **5**(1) (2001) 3–21.
7. M. M. Hörste and E. Schnieder, Formal modelling and simulation of train control systems using petri nets, in *FM '99: Proc. Wold Congress on Formal Methods in the Development of Computing Systems-Volume II* (Springer-Verlag, London, UK, 1999), p. 1867.
8. A. G. Hassami and A. G. Foord, Systems safety — A real example (european rail traffic management system, ERTMS), Second Int. Cont. Human Interfaces in Control Rooms, Cockpits and Command Centres, 2001, *IEE Conf. Publications*, No. 481 (2001), pp. 327–334.
9. P. di Tommaso, R. Esposito, P. Marmo and A. Orazzo, Hazard analysis of complex distributed railway systems, in *Proc. 22nd Int. Symposium on Hazand Analysis of Complex Distributed Railway Systems* (2003), pp. 283–292.
10. A. Zimmermann and G. Hommel, Towards modeling and evaluation of ETCS real-time communication and operation, *J. Syst. Softw.* **77**(1) (2005) 47–54.
11. J. Trowitzsch and A. Zimmermann, Using UML state machines and petri nets for the quantitative investigation of ETCS, in *valuetools'06: Proc. 1st Int. Conf. Performance Evaluation Methodolgies and Tools* (ACM, 2006), p. 34.

12. R. Esposito, A. Sanseviero, A. Lazzaro and P. Marmo, Formal verification of ERTMS Euroradio safety critical protocol, *IEEE Symp. on Formal Methods for Railway Operation and Control Systems* (IEEE Computer Society, 2003), pp. 21–29.
13. F. Flammini, S. Marrone, N. Mazzocca and V. Vittorini, Modelling system reliability aspects of ERTMS/ETCS by fault trees and bayesian networks, in *ESREL '06: Proc. 15th European Safety and Reliability Conf.* (*ESREL 2006*) (Taylor and Francis, 2006), 2675–2683.
14. F. Flammini, S. Marrone, N. Mazzocca and V. Vittorini, A new modeling approach to the safety evaluation of n-modular redundant computer systems in presence of imperfect maintenance, *Reliab. Eng. Syst. Saf.* **94** (2009) 1422–1432.
15. UNISIG, ERTMS/ETCS RAMS requirements specification, ref. 96s1266 (1998).
16. CENELEC, EN50126 railways applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS) (1999).
17. D. M. Nicol, W. H. Sanders and K. S. Trivedi, Model-based evaluation: From dependability to security, *IEEE Trans. Dependable. Secur. Comput.* **1**(1) (2004) 48–64.
18. P. J. Mosterman and H. Vangheluwe, Computer automated multi-paradigm modeling: An introduction, *Simulation* **80**(9) (2004) 433–450.
19. A. Joshi and M. P. E. Heimdahl, Behavioral fault modeling for model-based safety analysis, *IEEE Int. Symp. High-Assurance Systems Engineering* (2007), pp. 199–208.
20. V. Vittorini, M. Iacono, N. Mazzocca and G. Franceschinis, The OsMoSys approach to multi-formalism modeling of systems, *Softw. Syst. Model.* **3**(1) (2004) 68–81.
21. M. Iacono, E. Barbierato and M. Gribaudo, The SIMTHESys multiformalism modeling framework, *Comput. Math. Appl.* **64**(12) (2012) 3828–3839.
22. S. Bernardi, F. Flammini, S. Marrone, N. Mazzocca, J. Merseguer, R. Nardone and V. Vittorini, Enabling the usage of UML in the verification of railway systems: The DAM-rail approach, *Reliab. Eng. Syst. Saf.* **120** (2013) 112–126.
23. J. Peleska, J. Feuser and A. E. Haxthausen, The model-driven openETCS paradigm for secure, safe and certifiable train control systems, *Railway Safety, Reliability, and Security: Technologies and Systems Engineering* (IGI Global, Inc., 2012) 22–52.
24. F. Flammini, S. Marrone, N. Mazzocca, R. Nardone and V. Vittorini, Model-driven V&V processes for computer based control systems: A unifying perspective, in *Proc. 5th Int. Conf. Leveraging Applications of Formal Methods, Verification and Validation: Applications and Case Studies — Volume Part II* (Heraklion, Crete, Greece, 2012), pp. 190–204.
25. NUREG, *Fault Tree Handbook* (NUREG, 1981).
26. D. Codetta-Raiteri, M. Iacono, G. Franceschinis and V. Vittorini, Repairable fault tree for the automatic evaluation of repair policies, in *DSN '04: Proc 2004 Int. Conf. Dependable Systems and Networks* (IEEE Computer Society, Washington, DC, USA, 2004), p. 659.
27. A. Bobbio, L. Portinale, M. Minichino and E. Ciancamerla, Comparing fault trees and bayesian networks for dependability analysis, in *Proc. 18th Int. Conf. Computer Safety, Reliability and Security, SAFECOMP99* (1999), pp. 310–322.
28. The world of ERTMS, Available at: http://www.ertms.com/.
29. F. Flammini, N. Mazzocca, M. Iacono and S. Marrone, Using repairable fault trees for the evaluation of design choices for critical repairable systems, *IEEE Int. Symp. High-Assurance Systems Engineering* (2005), pp. 163–172.
30. S. Bernardi and S. Donatelli, Building petri net scenarios for dependable automation systems, in *Proc. 10th Int. Workshop on Petri Nets and Performance Models* (*PNPM2003*) (IEEE Computer Society, 2003), pp. 72–81.

31. G. Bucci, L. Sassoli and E. Vicario, Correctness verification and performance analysis of real-time systems using stochastic preemptive time petri nets, *IEEE Trans. Softw. Eng.* **31**(11) (2005) 913–927.
32. K. Goseva-Popstojanova and K. S. Trivedi, Stochastic modeling formalisms for dependability, performance and performability, in *Performance Evaluation: Origins and Directions* (Springer-Verlag, London, UK, 2000), pp. 403–422.
33. R. German, *Performance Analysis of Communication Systems with Non-Markovian Stochastic Petri Nets* (John Wiley & Sons, Inc., New York, NY, USA, 2000).
34. F. Gagliardi Cozman, JavaBayes — User manual, Available at: http://www.cs.cmu.edu/∼javabayes/.
35. F. Moscato, F. Flammini, G. Di Lorenzo, V. Vittorini, S. Marrone and M. Iacono, The software architecture of the osmosys multisolution framework, in *ValueTools '07: Proc. 2nd Int. Conf. Performance Evaluation Methodologies and Tools* (ICST, Brussels, Belgium, 2007), pp. 1–10.

About the Authors

Francesco Flammini got with honors his laurea (2003) and doctorate (2006) degrees in Computer Engineering from the University Federico II of Naples. Since October 2003, he has worked in Ansaldo STS (Finmeccanica) on the safety and security of transit infrastructures. He has taught Computer Science and Software Engineering as an Adjunct Professor as well as seminars on computer dependability and critical infrastructure protection in post-degree courses on Homeland Security. He has co-authored several books and more than 50 scientific papers published in international journals and conference proceedings. He has served as the chairman, a PC member and an editor for several international conferences and journals. He is a Senior Member of the IEEE and an ACM Distinguished Speaker.

Stefano Marrone is an Assistant Professor in Computer Engineering at Seconda Università di Napoli. He formerly worked in AnsaldoSTS as V&V and software testing specialist. His interests include the definition of model driven processes for the design and analysis of critical systems, in particular transportation control systems, complex communication networks and critical infrastructures protection. He authored about 40 scientific papers published in both international journals and in proceedings of international conferences. He participates in several national and international research projects with both academic and industrial partners.

Mauro Iacono is a tenured Assistant Professor and Senior Researcher in Computing Systems. He received a Laurea in Ingegneria Informatica (M.Sc) degree cum laude in 1999 by Universit degli Studi di Napoli "Federico II", Napoli, Italy, and a Dottorato in Ingegneria Elettronica (Ph.D) degree by Seconda Universit degli Studi di Napoli, Aversa, Italy. He published over 40 peer reviewed scientific papers on international journals, books and conferences and has served as scientific editor, conference scientific committee chairman and member and reviewer for several journals, and is a member of IEEE and other scientific societies. His research activity is mainly centered on the field of performance modeling of complex computer-based

systems, with a special attention for multiformalism modeling techniques, critical systems and Big Data systems.

Nicola Mazzocca is a Full Professor of Computer Engineering at the head of the Department of "Ingegneria Elettrica e Tecnologie dell'Informazione" University of Naples "Federico II". He authored over 270 papers on international journals, books and conferences. His research activities are mainly centered on computer architecture, dedicated systems, reliable and secure systems, performance evaluation in high-performance systems.

Valeria Vittorini is an Associate Professor at the University of Naples Federico II (Italy). She teaches Fundamentals of Computer Systems, Computer Programming and Formal Methods at the Department of "Ingegneria Elettrica e Tecnologie dell'Informazione". Her current research interests are in the area of dependability and performance evaluation of computer systems, critical infrastructures modeling and physical security. She is Associate Editor of the *International Journal of Critical Computer Based Systems*.