Simulation Modelling Practice and Theory 47 (2014) 1–18

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Availability assessment of railway signalling systems with uncertainty analysis using Statecharts

S. Qiu [a], M. Sallak [a,*], W. Schön [a], Z. Cherfi-Boulanger [b]

[a] Computer Science Department, Compiegne University of Technology, Heudiasyc Laboratory, UMR 7253, CNRS, Research Center of Royallieu, France
[b] Department of Mechanics, Compiegne University of Technology, Heudiasyc Laboratory, UMR 7253, CNRS, Research Center of Royallieu, France

ARTICLE INFO

Article history:
Received 29 October 2013
Received in revised form 20 April 2014
Accepted 21 April 2014

Keywords:
Railway signalling system
Statecharts
Availability
ERTMS/ETCS Level 2
Belief functions theory
State uncertainty

ABSTRACT

In this paper, we propose an original simulation approach to evaluate the availability of systems in the presence of state uncertainty which arises from incompleteness or imprecision of knowledge and data. This approach is based on a simulation method combining the belief functions theory and the Statecharts. Then we propose a Statechart model of a railway signalling system, European Rail Traffic Management System (ERTMS) Level 2 considering state uncertainty, and evaluate its availability according to the RAMS requirements defined in the railway standards. Finally we propose a sensitivity analysis to estimate the state uncertainty of which constituent system has the most significant influence on the state uncertainty of the entire ERTMS Level 2.

1. Introduction

The safety of railway systems is very important, because railway accidents/incidents usually cause enormous losses. The improvement of the availability of systems is always a significant goal in railway systems. Availability is the ability of a system to be in a state to perform a required function under given conditions at a given instant of time. It is computed by the proportion of time a system is functioning [1,2]. A safety analysis assesses the level and consequences of failures on the users and the system. Both of them are attributes of RAMS (Reliability, Availability, Maintainability, Safety) and can be used to evaluate the performance of a system. In this paper, a railway signalling system which is used to control railway traffic is studied. This railway signalling system is ERTMS Level 2.

Several models of ERTMS have been proposed in the literature. Hermanns et al. [3] used StoCharts to model European Train Control System (ETCS) and evaluate the dependability of the train radio system. StoCharts are the Quality of Service (QoS)-oriented extension of Unified Modeling Language (UML) Statecharts. They lack tool support, so they are translated into the Modeling and Description Language for Stochastic and Timed Systems (MoDeST) which is a formal language used for describing stochastic timed systems. Vernez and Vuille [4] have proposed a functional Failure Mode, Effects and Criticality Analysis (FMECA) approach to optimize the dependability of ERTMS Level 2. Lalouette et al. [5] have proposed an approach based on Coloured Petri Nets to evaluate the dependability of ERTMS. Beugin and Marais [6] have used RAMS attributes to evaluate the solutions of satellite-based localization services in the ERTMS. Herranz et al. [7] have modeled ERTMS/ETCS using UML diagrams and then transformed their UML models into Uppaal (integrated tool environment for modeling,

* Corresponding author. Tel.: +33 0344234930.
E-mail addresses: siqi.qiu@utc.fr (S. Qiu), sallakmo@utc.fr (M. Sallak), walter.schon@utc.fr (W. Schön).

http://dx.doi.org/10.1016/j.simpat.2014.04.004
1569-190X/

validation and verification of real-time systems) specifications. European Railway Agency [8] has funded a European Railway Formalization and Validation Project which has proposed the use of Rational tools for the formalization and validation of ETCS specifications. Bernardi et al. [9] and Flammini et al. [10] have proposed an architecture schema of ERTMS Level 2 and evaluated its reliability by Fault Trees, Bayesian Networks and some UML diagrams. Zimmermann and Hommel [11] have used Stochastic Petri Nets to model and evaluate the failure and recovery behavior of the communication link as well as its combination with the exchange of vital train information between trains and radio block centers. None of the works cited has provided a complete model that takes all the constituents of the ERTMS into account while at the same time taking its dynamic behavior into account. This has been our motivation in proposing our own model.

Furthermore, previous ERTMS models have not taken uncertainties into account. Zhang and Mahadevan [12] summarized three types of sources for the uncertainty in engineering analysis: (1) Physical uncertainty or inherent variability which is generally quantified by a probability distribution estimated from observed data. (2) Statistical uncertainty which is the uncertainty in the statistical distribution parameters of the random variables due to the insufficiency of data. (3) Modeling uncertainty which exists in model accuracy and model selection. According to Nilsen and Aven [13], model uncertainty is commonly related to deviations between the real world and its representation in models. These deviations come from two sources: the limitation of modeler's knowledge and the deliberate simplification introduced by the modeler. Indeed, during the last years, the reliability and risk assessments community has recognized that there are different sources/type s of uncertainties that play an important role in reliability and risk evaluation [14,15]. In the work of Aven [16], uncertainties are usually divided into two types: aleatory uncertainty which is represented by probability models and frequentist probabilities, and epistemic uncertainty which expresses the lack of knowledge about the true values of the frequentist probabilities and parameters of probability models. The distinction is important because epistemic uncertainty can be reduced by acquiring knowledge on the studied system, whereas aleatory uncertainty cannot. Furthermore, some works have proven that uncertainties in reliability and risk assessments are mainly epistemic [17]. A real model of ERTMS Level 2 is proposed in this paper. In rail transport, accident data are scarce due to the rare occurrence of accidents [18]. The incompleteness of data brings epistemic uncertainty into the model.

Keep in mind that there are other points of view as to how to distinguish sources or types of uncertainty [19,20]. As a consequence, several theories were presented, including Bayesian theory, imprecise probability theory [21], possibility theory [22,23], belief functions theory [24,25], etc. The Bayesian approach requires us to specify probability distribution about component state. But, in many cases, prior knowledge is either vague, or non-existent. We propose the use of belief functions theory because it is well adapted to model the imprecision of system state by quantifying the belief masses of component state provided by experts. During the last years, belief functions theory was applied to do reliability and risk analysis [26–29]. In our knowledge, there is no work in the literature, which is related to the evaluation of the availability of systems considering epistemic uncertainty by belief functions theory, in reliability and risk studies.

In this work we propose modeling the behavior of ERTMS Level 2 using Statecharts. While modeling systems in Statecharts, two kinds of epistemic uncertainties may exist: parametric uncertainty which exists in the transition rates and state uncertainty which exists in the states. Parametric uncertainty means there is imprecision of the values of parameters. In the model, values of some parameters may come from the statistics, from systems which have the similar functionality or from experts' opinions, so these parameters are imprecise. The imprecision makes parametric uncertainty analysis necessary in modeling systems. Many researchers have studied the parametric uncertainties in modeling systems [17,39,40]. In this paper, the parametric uncertainty is not handled. The focus is the state uncertainty. State uncertainty means there is imprecision of the states of systems. In other words, sometimes the states of systems are uncertain. It is caused b y the lack of information about components of systems and it represents the ignorance about the states of systems. The state uncertainty is epistemic. Epistemic state uncertainty has not been modeled and quantified by belief functions theory in the literature before.

Due to the environment and the lack of failure data (due to rare events failures) related to some components or subsystems used in railway systems, there are epistemic uncertainties when modeling such systems. Indeed, state uncertainties represent the part of uncertainties related to the states of these components. Their existence influences the values of RAMS parameters of ERTMS. Furthermore, the availability requirements of ERTMS are very strict because railway accidents always bring in huge losses. Thus, to estimate the railway system's availability, the influence brought by such uncertainties should be taken into account. Thus, the main objective of this paper is to evaluate the availability of railway signalling systems taking epistemic state uncertainty into account.

The remainder of this paper is organized as follows. The use of the belief functions theory to formalize state uncertainties of systems is introduced in Section 2. Section 3 presents Statecharts and proposes two approaches to evaluate the availability of binary components considering state uncertainty. In Section 4, an application based on the railway signalling system ERTMS/ETCS Level 2 considering state uncertainty is detailed. Section 5 concludes this paper.

2. Use of the belief functions theory to formalize state uncertainties of systems

The theory of belief functions (also known as Demspter–Shafer theory and evidence theory) originated with the work of Dempster in the 1960s [24,41]. Dempster developed a generalization of the Bayesian theory of subjective probabilities based on the upper and lower probabilities induced from a multivalued mapping. Glenn Shafer further extended Dempster's work

into a general theory of evidence. He introduced belief functions and their construction from degrees of belief, in his book *A Mathematical Theory of Evidence*, published in 1976 [25].

As explained by Shafer [25]: '*belief functions allow us to base degrees of belief for one question from probabilities for another. These degrees of belief may or may not have the mathematical properties of probabilities; how much they differ from probabilities will depend on how closely the two questions are related.*' Suppose that an expert X is asked to indicate if a component c is working perfectly or not. The degree of belief that X is absolutely trustworthy is 0.9, and the degree of belief that X is not trustworthy is 0.1. Let us consider the fact that X indicates that c is perfectly working. This information, which must be true if X is trustworthy, is not necessarily false if X is not trustworthy. There is a 0.9 degree of belief that c is perfectly working, but only a 0 degree of belief (not a 0.1 degree of belief) that c is down. Thus, the belief interval that c is working perfectly is [0.9,1], and the belief interval that c is down is [0,0.1]. The length of the belief interval 0.1 represents the epistemic uncertainty (the imprecision) about the state of c. The values 0.9 and 1 represent the bounds of the correct value of being in the working state (aleatory uncertainty). Thus, we have obtained degrees of belief for one question (the state of c) from probabilities of another question (the trustworthiness of X). Note that whereas subjective probabilities are additive, belief functions are only super-additive.

In this section, we give a brief introduction to the theory of belief functions.

A frame of discernment $\mathcal{X}$ represents the finite set of possible answers to some questions, one and only one of which is correct. A function $m : 2^{\mathcal{X}} \to [0,1]$ is said to be a basic belief assignment on the measurable space $(\mathcal{X}, 2^{\mathcal{X}})$ if it satisfies $\forall E \in 2^{\mathcal{X}}$, $\sum_{E \subseteq \mathcal{X}} m(E) = 1, m(E) \geqslant 0$, and $m(\emptyset) = 0$.

The theory of evidence assigns a belief mass to each element of the power set. The basic belief assignment $m(E)$ reflects the degree of belief (subjective probability) committed to that part of the information which exactly points to E and cannot be divided among subsets of E.

For example, consider a binary component i which can be in either of two states:

- a completely working state, denoted by 0_i;
- a failed state, denoted by 1_i.

The frame of discernment of the component i is given by $\mathcal{X}_i = \{0_i, 1_i\}$. A subset E of $\mathcal{X}$ such that $m(E) > 0$ is said to be a focal element. For every belief mass m, call $\mathcal{F}_m$ the set of focal elements of m. Note that several subclasses of belief functions can be characterized just by the structure of $\mathcal{F}_m$. In particular, when $\mathcal{F}_m = x, x \in \mathcal{X}$, we obtain a probability measure.

Given a set $\mathcal{X}$ and a basic belief assignment m on $(\mathcal{X}, 2^{\mathcal{X}})$, for every $A \in 2^{\mathcal{X}}$, the belief function of A is defined as the sum of all the masses that support A. It is computed as follows [25]

$$Bel(A) = \sum_{E|E \subseteq A} m(E) \tag{1}$$

The plausibility function of A represents the total amount of masses that might support A. It is computed as follows [25]

$$Pl(A) = \sum_{E|E \cap A \neq \emptyset} m(E) = 1 - Bel(\overline{A}) \tag{2}$$

For example, consider an expert who gives his degree of belief about the event A: "*the component i is in the working state at time t*", in the form $[Bel(0_i), Pl(0_i)] = [0.7, 0.9]$. The value 0.7 represents the total amount of information that implies the event A, whereas the value 0.9 represents the total amount of information which does not contradict the event A according to the expert. The length of the interval $Pl(0_i) - Bel(0_i) = 0.2$ represents the expert's epistemic uncertainty (imprecision) about the working state of component. However, the degrees of belief and plausibility should not be interpreted as lower and upper bounds on some unknown true probability because belief functions are not, in general, related to a well-defined reference population with learning about the frequencies in this population. They express subjective judgment of experts.

Note that a belief mass m can equivalently be represented through a set of probability measures such that

$$\mathcal{P}(m) = \{P \in \mathbb{P}_{\mathcal{X}} \forall A \subseteq \mathcal{X}, Pl(A) \geqslant P(A) \geqslant Bel(A)\} \tag{3}$$

where $\mathbb{P}_{\mathcal{X}}$ is the set of all the probabilities on $\mathcal{X}$ that are compatible with the belief and plausibility functions. Thus, associated to each belief function, there is a closed convex set of probability measures of which a belief function is a lower bound.

Several studies proved that the belief functions theory is well adapted to represent epistemic uncertainty in reliability analysis [16,42]. An example which applies belief functions theory on the availability analysis of a component is given below. The availability A of a component at time T is the probability of the event E: "*the component will operate satisfactorily at a given point in time when used under stated conditions*". The belief function is a lower bound on the probability of the event E. The corresponding upper bound is called plausibility function. Thus, belief and plausibility should bracket availability. Note that not all upper and lower probability models correspond to belief functions. Belief function imposes a further restriction called total monotonicity property, i.e. for every $n \geqslant 2$ and a collection of $A_1, \ldots, A_n \in 2^{\mathcal{X}}$ [25]

$$Bel(\cup_{i=1}^{n} A_i) \geqslant \sum_{\emptyset \neq I \subset \{1,\ldots,n\}} (-1)^{|I|+1} Bel(\cap_{i \in I} A_i) \tag{4}$$

This property of total monotonicity indicates that belief measures do not verify the inclusion–exclusion principle [25].

For example, let us consider a binary component i which fails according to a Poisson process. An expert is asked to provide a bounding interval for the failure rate of the component λ such that $\lambda \in [\underline{\lambda}, \overline{\lambda}]$. We aim to shown how to obtain belief and plausibility values of the component availability from the upper and lower values given by the expert.

Let T be the amount of time when the component i must function for the system to succeed, and we let w be the lifetime of the component. The process is Poisson, thus the variable w follows an exponential distribution with scale parameter $1/\lambda$. Then the variable $v = \lambda w$ follows a unit exponential distribution. The component will fail during operation when $w \leqslant T$, or $\lambda \geqslant v/T$. Let F be an indicator variable of component failure. If $v/T \leqslant \underline{\lambda}$, then the component will certainly fail, i.e.

$$Bel(F = 1)(T) = 1 - exp(-\underline{\lambda}T)$$

Similarly, if $v/T \leqslant \overline{\lambda}$, the component may fail, i.e.

$$Pl(F = 1)(T) = 1 - exp(-\overline{\lambda}T)$$

The unavailability U_i of the component i at time T is then given by:

$$Bel(U_i(T)) = 1 - exp(-\underline{\lambda}T) \leqslant U_i(T) \leqslant Pl(U_i(T)) = 1 - exp(-\overline{\lambda}T)$$

Finally, the availability A_i of the component i at time T is given by:

$$Bel(A_i(T)) = e^{-T\overline{\lambda}} \leqslant A_i(T) \leqslant Pl(A_i(T)) = e^{-T\underline{\lambda}} \tag{5}$$

In this paper, epistemic state uncertainty represents the imprecision of the states. It is well represented by belief functions theory and can be quantified by belief masses. Because of the state uncertainty, the availability of the ERTMS Level 2 is imprecise. As the state uncertainty can be quantified by belief masses, the availability of the ERTMS Level 2 taking epistemic state uncertainty into account can be assessed by an interval made up of belief and plausibility measures.

3. Approach proposed to model state uncertainties in availability studies

In this section, first of all, the principal elements of Statecharts are presented. Then, we propose two approaches to evaluate the availability of binary components which takes the epistemic state uncertainty into account.

3.1. Statecharts

Statecharts use states and state transitions to describe the behavior of systems. They specify the sequences of states that systems go through as a result of the occurrences of events and their corresponding actions [30–35]. Furthermore, Statecharts introduce new concepts such as the hierarchy of states and orthogonal regions. They also extend actions that depend on states. In fact, Statecharts have been widely used in research into the modeling of railway systems. Banci et al. [36] used Statecharts to give precise specifications on a computer controlling Railway Interlocking system. To develop tools and techniques which can check automatically whether railway equipment conforms to operational requirements, Herranz et al. [7] used Statecharts to model the ERTMS/ETCS specifications. Pap et al. [37] presented methods and tools for checking general safety criteria in UML Statecharts relating to safety–critical systems. Magott and Skrobanek [38] introduced fault trees with time dependencies and timed Statecharts for carrying out timing analysis of safety properties in safety critical systems.

Here we present the principal elements to be found in Statecharts [31,43].

- A **state** models a situation that a system might be in. A state which contains other states is called a composite state. Each state may have Entry, During and Exit actions.
- **Exclusive (OR) states** represent mutually exclusive modes of operation.
- **Parallel (AND) states** represent independent modes of operation.
- A **transition** is the relationship between a source state and its target state. Exclusive (OR) states require transitions. Parallel (AND) states do not require transitions because they execute concurrently.
- A **region** is an orthogonal part of a Statechart or a composite state. A Statechart or a composite state can contain one or more regions. When a state contains two or more regions, these regions are said to be orthogonal. If a Statechart has several regions, these regions are concurrent.
- A **default transition** indicates which exclusive (OR) state is to be active when there is ambiguity between two or more exclusive (OR) states at the same level in the hierarchy.
- **State actions** are actions executed based on the status of a state.
  - **Entry** action is optional and performed whenever the state is entered.
  - **Exit** action is optional and performed whenever the state is exited.
  - **During** action is optional and executed when the state is active and no valid transition to another state is available. It is performed after the completion of the Entry action and continues to be performed until the action has finished or the state is exited.
- **Conditions** are expressions enclosed in square brackets that evaluate to true or false.
- **Events** are objects that trigger activities during the execution.

Fig. 1 is an illustration of a Statechart diagram. The system has three states. It first enters State1, which has Entry, During and Exit actions. The system passes from State1 to State2 when Event1 is triggered and where the Condition is satisfied. State2 has two parallel sub-states. This means that State2.1 and State2.2 are both active when the system enters State2. When Event2 is triggered, the system enters State3. When Event3 is triggered, the system returns to State1.

Over the years, several Statechart semantics have been proposed in the literature such as: Statemate, UML Statecharts, Rhapsody Statecharts, Stateflow, and SyncCharts. In this paper, we use Stateflow which is one of the most popular Statecharts dialects. It includes particularly some complicated features such as: interlevel transitions, complex transitions through junctions, and events broadcasting. We use the MATLAB Simulink/Stateflow tool. MATLAB Simulink is a graphical notation that supports the specification of control systems at a level of abstraction convenient for engineers. Stateflow is a part of Simulink, and consists of a Statechart notation used to define Simulink blocks.

3.2. Availability of binary components without state uncertainty

A binary component can be in either of two states (working or failed) at any given time. Given that the failure rate and the repair rate are constant, the component availability can be derived by the probabilistic approach. The component availability $A_i(t)$ is defined as the probability of being in the working state at time t.

Fig. 2(a) shows the Markov model of a binary component. "0" denotes the working state and "1" denotes the failed state. The transition probability can be represented by the product of the transition rate and the simulation step Δt when Δt is suitably small. Thus, the transition probability from the working state to the failed state is $\lambda * \Delta t$ and the transition probability from the failed state to the working state is $\mu * \Delta t$, where λ is the failure rate, μ is the repair rate and Δt is the simulation step. Fig. 2(b) shows the corresponding Statechart of this binary component.

The availability of being in the working state and in the failed state is given in Eq. (6). The derivation of Eq. (6) is detailed in the Appendix. The component availability $A_i(t)$ is $A_0(t)$.

$$\begin{cases} A_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \\ A_1(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \end{cases} \tag{6}$$

Note that, as usual in availability evaluation, we can consider "steady-state" availability as the limit for $t \to$ infinite, obtaining an absolute number, which is the one that is usually confronted with availability requirements.

3.3. Availability of binary components considering state uncertainty

In this subsection, the state uncertainty is introduced into the binary component model.

Based on the definition of belief functions, the frame of discernment of the binary component state is $\mathcal{X} = \{0, 1\}$. The component state takes value in $2^{\mathcal{X}} = \{\emptyset, \{0\}, \{1\}, \mathcal{X}\}$. The elements in this power set represent separately that the component is in neither of the two states, the component is in the working state, the component is in the failed state or its state is

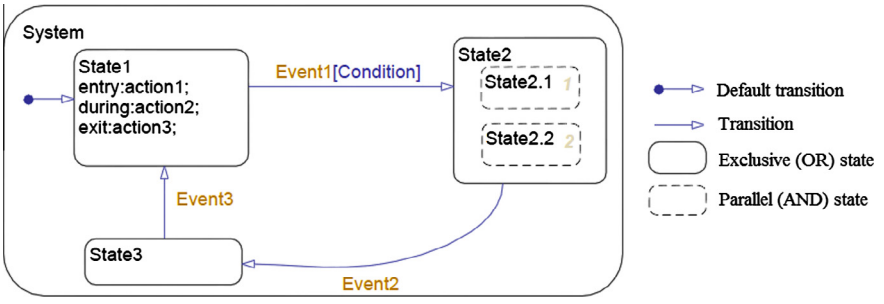


Fig. 1. Illustration of a Statechart diagram.

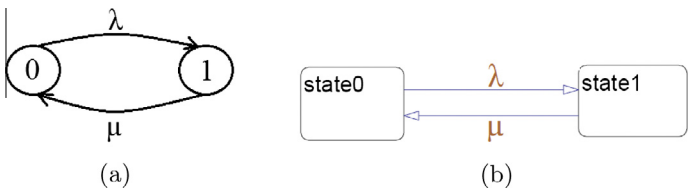


Fig. 2. Models of a binary component. (a) Markov model. (b) Statechart.

uncertain. To develop the Markov model of the binary component considering state uncertainty, we assume a fictive state that represents the imprecision. This fictive state is not a true state. It represents the imprecision of the component state. A belief mass is assigned to each element of the power set $2^{\mathcal{X}}$. The meanings of these masses are listed here:

- $m(\emptyset)$ Represents the degree of belief that the component is in neither of the two states.
- $m(\{0\})$ Represents the degree of belief that the component is the working state.
- $m(\{1\})$ Represents the degree of belief that the component is the failed state.
- $m(\mathcal{X})$ Represents the degree of belief that the component is in either of the two states, but we cannot confirm exactly its state.

Here we have $m(\emptyset) = 0$ and $m(\{0\}) + m(\{1\}) + m(\mathcal{X}) = 1$. These mean that the component state must be in the frame of discernment.

Fig. 3(a) shows the Markov model of the binary component considering state uncertainty and Fig. 3(b) shows its corresponding Statechart. We assume that when the component is in the working state or in the failed state, it has a chance to go into the fictive state. In practice, components are examined at specified-time intervals. If the state of a component is found to be uncertain during an examination, a more deep analysis should be performed. If we succeeded in this analysis, we will repair the component if it is failed, or we will leave it in its uncertainty state if we cannot know its state. A deep analysis should never degrades the state of the component (the next state of a component in an uncertainty state should be never a failed state). Thus, the next state of fictive state is supposed to only be the working state.

The transition probability from the working state to the failed state is $\lambda * \Delta t$, the transition probability from the failed state to the working state is $\mu * \Delta t$, the transition probability from the working state to the fictive state is $\epsilon_{0\lambda} * Deltat$, the transition probability from the fictive state to the working state is $\epsilon_{0\mu} * \Delta t$, the transition probability from the failed state to the fictive state is $\epsilon_{1\mu} * \Delta t$, where λ is the failure rate, μ is the repair rate, Δt is the simulation step, $\epsilon_{0\mu}, \epsilon_{1\mu}$ and $\epsilon_{0\lambda}$ are transition rates related to the fictive state. The values of $\epsilon_{0\mu}, \epsilon_{1\mu}$ and $\epsilon_{0\lambda}$ are estimated by counting the times that the state of a component becomes uncertain from past experience. In practice, they are provided by railway experts.

According to Fig. 3(a), there are three states in the Markov model: a working state, a failed state and a fictive state. According to Fig. 3(b), there are also a working state, a failed state and a fictive state in the Statechart. The transitions and transitions rates among the three states in the two models are all the same. The difference between the two models lies in the representation of the initial conditions. In the Markov model, initial conditions are not represented graphically. However in the Statechart, initial conditions are represented graphically by two temporary states and two time constants.

In the proposed analytic approach, mass functions are used to measure the availability of system states and the mass functions are functions of time. From the Markov model in Fig. 3(a), we have the following equations

$$\begin{cases} m(\{0\})(t+\Delta t) = m(\{0\})(t) * (1 - \lambda\Delta t - \epsilon_{0\lambda}\Delta t) + m(\{1\})(t) * \mu\Delta t + m(\mathcal{X})(t) * \epsilon_{0\mu}\Delta t \\ m(\{1\})(t+\Delta t) = m(\{1\})(t) * (1 - \mu\Delta t - \epsilon_{1\mu}\Delta t) + m(\{0\})(t) * \lambda\Delta t \end{cases} \tag{7}$$

where $m(\{0\})(t) + m(\{1\})(t) + m(\mathcal{X})(t) = 1$.

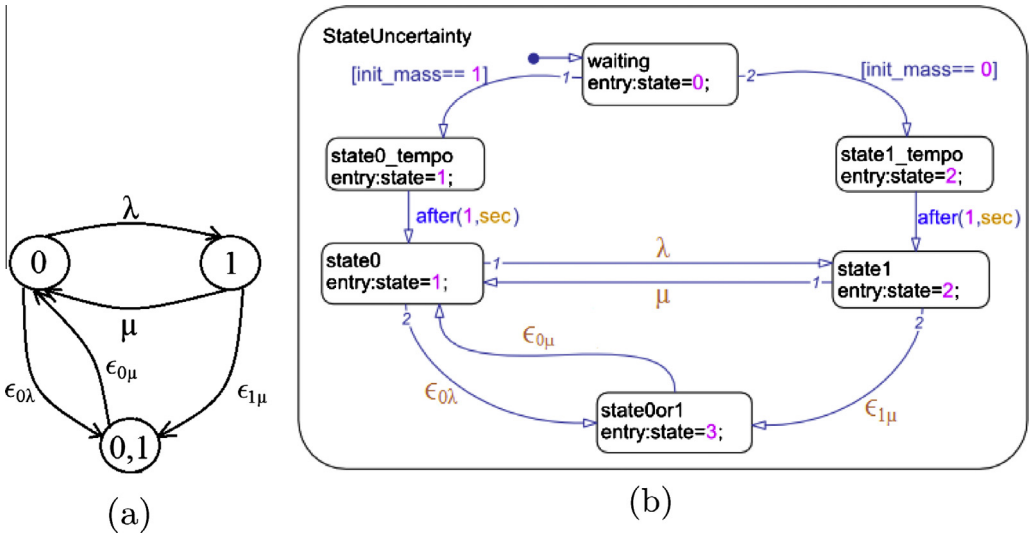


Fig. 3. Models of a binary component considering state uncertainty. (a) Markov model. (b) Statechart.

To facilitate the expressions of the solutions of Eq. (7), we suppose $a_1 = -\lambda - \epsilon_{0\lambda} - \epsilon_{0\mu}, b_1 = \mu - \epsilon_{0\mu}, c_1 = \epsilon_{0\mu}$, $a_2 = \lambda, b_2 = -\mu - \epsilon_{1\mu}, k_{1,2} = \frac{a_1+b_2 \pm \sqrt{(a_1-b_2)^2+4a_2b_1}}{2}$. The solutions of Eq. (7) are given as follows. The derivation of the solutions is detailed in the Appendix.

- If $(a_1 - b_2)^2 + 4a_2b_1 > 0$

$$\begin{cases} m(\{0\})(t) = n_1 e^{k_1 t} + n_2 e^{k_2 t} - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ m(\{1\})(t) = m_1 e^{k_1 t} + m_2 e^{k_2 t} + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{8}$$

- If $(a_1 - b_2)^2 + 4a_2b_1 = 0$

$$\begin{cases} m(\{0\})(t) = (n_1 + n_2 t) e^{k_1 t} - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ m(\{1\})(t) = (m_1 + m_2 t) e^{k_1 t} + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{9}$$

- If $(a_1 - b_2)^2 + 4a_2b_1 < 0$

$$\begin{cases} m(\{0\})(t) = e^{\alpha t}(n_1 \cos \beta t + n_2 \sin \beta t) - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ m(\{1\})(t) = e^{\alpha t}(m_1 \cos \beta t + m_2 \sin \beta t) + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{10}$$

where α and β come from $k_{1,2} = \alpha \pm i * \beta$.

n_1, n_2, m_1, m_2 are unknown. Initial conditions are needed to fix their values.

Based on the above solutions, if the values of $\lambda, \mu, \epsilon_{0\lambda}, \epsilon_{0\mu}, \epsilon_{1\mu}$ and initial conditions are given, we can obtain the expressions of $m(\{0\})(t), m(\{1\})(t)$ and $m(\mathcal{X})(t)$. And from the knowledge of belief functions, the availability of the component considering state uncertainty should belong to $[Bel(\{0\}), Pl(\{0\})]$, where

$$\begin{cases} Bel(\{0\}) = m(\{0\})(t) \\ Pl(\{0\}) = m(\{0\})(t) + m(\mathcal{X})(t) \end{cases} \tag{11}$$

Example Here is a numerical example for the binary component considering state uncertainty. In this example, the values of all the transition rates are known as follows

$$\begin{cases} \lambda = 0.03\ \mathrm{h}^{-1} \\ \mu = 0.02\ \mathrm{h}^{-1} \\ \epsilon_{0\lambda} = 0.03\ \mathrm{h}^{-1} \\ \epsilon_{0\mu} = 0.03\ \mathrm{h}^{-1} \\ \epsilon_{1\mu} = 0.03\ \mathrm{h}^{-1} \end{cases} \tag{12}$$

These transition rates have their own meanings. For instance, the $\epsilon_{0\lambda} * \Delta t$ is the transition probability of entering into the fictive state from the working state. In this application, it represents the probability with which the component enters into the fictive state from the working state. For example, $\epsilon_{0\lambda} * \Delta t = 0$ means it is impossible that the state of the component becomes uncertain when the component is in the working state. So $\epsilon_{0\lambda} * \Delta t = 0.03$ means that when the component is in the working state, the probability with which the state of the component becomes uncertain is 0.03.

Scenario 1: Without state uncertainty in the initial conditions

To calculate the component availability, two initial conditions are given: $m(\{0\})(0) = 0.8$ and $m(\{1\})(0) = 0.2$. There is no state uncertainty in the initial conditions. The values in Eq. (12) are put into Eq. (8). With the initial conditions, the solutions of scenario 1 are obtained as follows

$$\begin{cases} m(\{0\})(t) = a * e^{-0.06*t} + (0.4875 - a) * e^{-0.08*t} + 0.3125 \\ m(\{1\})(t) = b * e^{-0.06*t} + (0.0125 - b) * e^{-0.08*t} + 0.1875 \\ m(\mathcal{X})(t) = 0.5 - (a + b) * e^{-0.06*t} - (0.5 - a - b) * e^{-0.08*t} \end{cases} \tag{13}$$

where a and b are two unknown parameters, because the two initial conditions are not sufficient to fix the solutions.

$m(\{0\})(0)$ represents the degree of belief that the component is in the working state at time $t = 0$. $m(\{1\})(0)$ is the degree of belief that the component is in the failed state at $t = 0$. $m(\mathcal{X})(0)$ represents the degree of belief that the component is in either of the two states at $t = 0$, but we cannot confirm exactly its state.

In belief function theory, the masses can be affected to singletons ($\{0\}$ and $\{1\}$) and subset ($\mathcal{X} = \{0, 1\}$) of states whereas the probabilities can be affected only to singletons of states.

The initial conditions in the Statechart are realized by introducing an initial probability to the entrance of each state. We simulate the Statechart of the binary component considering state uncertainty with the above values in Stateflow. The simulation results of the Statechart and the analytic results of Eq. (13) are given in Fig. 4(a).

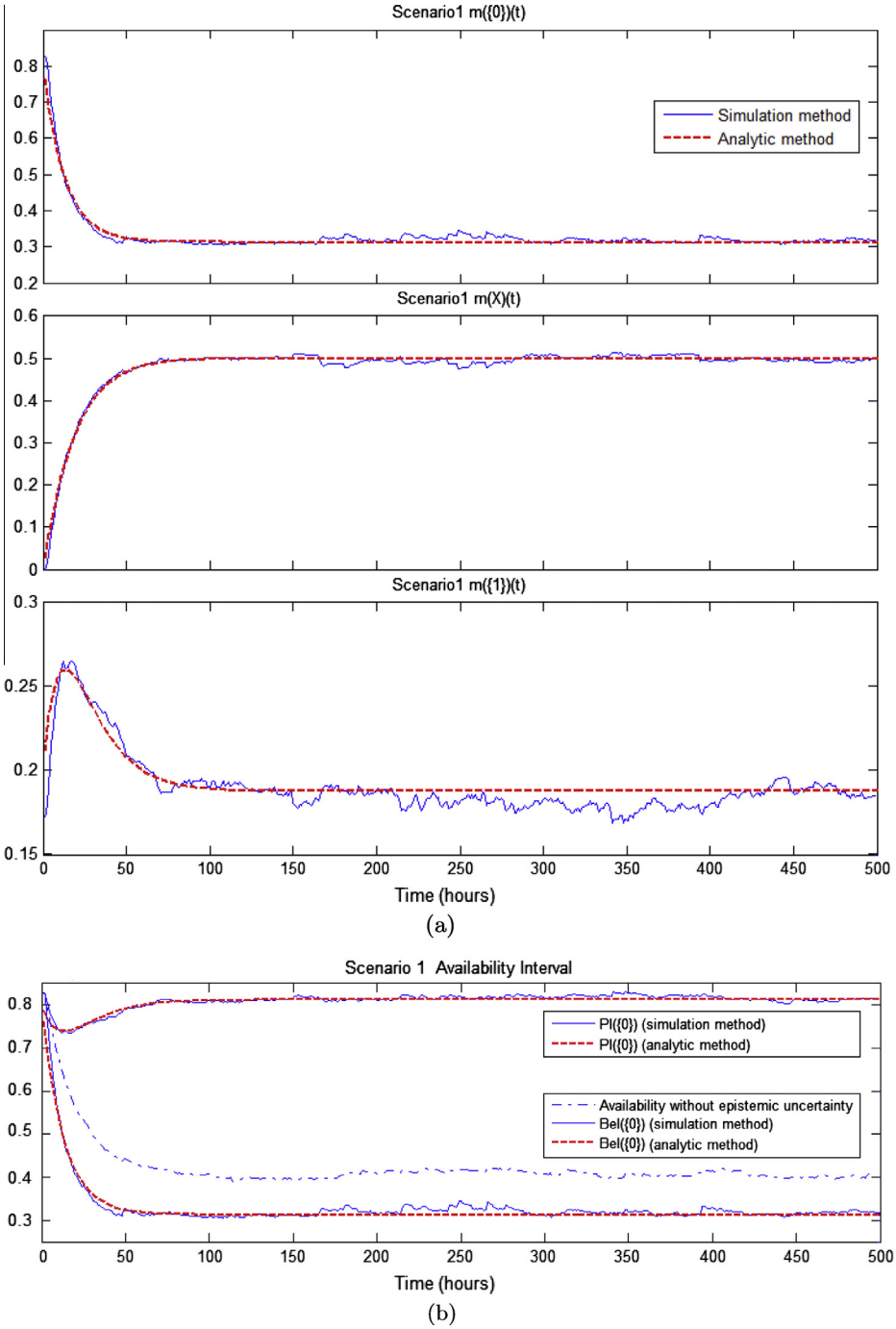


Fig. 4. Simulation results and the analytic results of scenario 1. (a) Basic probability assignments. (b) Availability interval and the accurate availability.

Fig. 4(b) shows the simulation result and the analytic result of the availability interval of the binary component considering state uncertainty in scenario 1. The simulation result of the availability of the binary component without epistemic state uncertainty ($\epsilon_{0\lambda} = \epsilon_{0\mu} = \epsilon_{1\mu} = 0$) is also drawn in this figure. Obviously, the availability without epistemic state uncertainty is included in the availability interval. From Fig. 4, we find that the simulation result is very close to the analytic result.

Scenario 2: With state uncertainty in the initial conditions

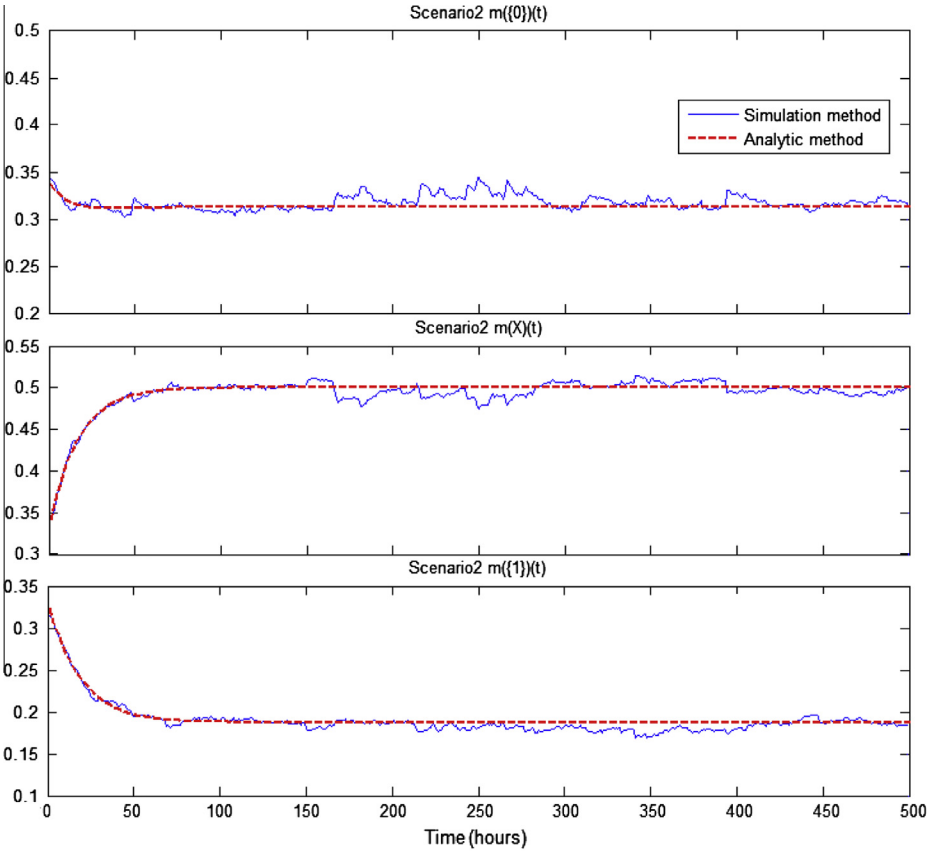
In this scenario, three initial conditions are given: $m(\{0\})(0) = 0.34, m(\{1\})(0) = 0.33$ and $m(\mathcal{X})(0) = 0.33$. It means that there is state uncertainty in the initial conditions. In this scenario, $m(\{0\})(0)$ is the mass of passing from "**waiting**" state to "**state0_tempo**". $m(\{1\})(0)$ is the mass of passing from "**waiting**" state to "**state1_tempo**". Thus $m(\mathcal{X})(0) = 1 - m(\{0\})(0) -$

$m(\{1\})(0)$ is the initial mass that the state of the component is unknown. As the state is unknown, the component stays in "**waiting**" state.

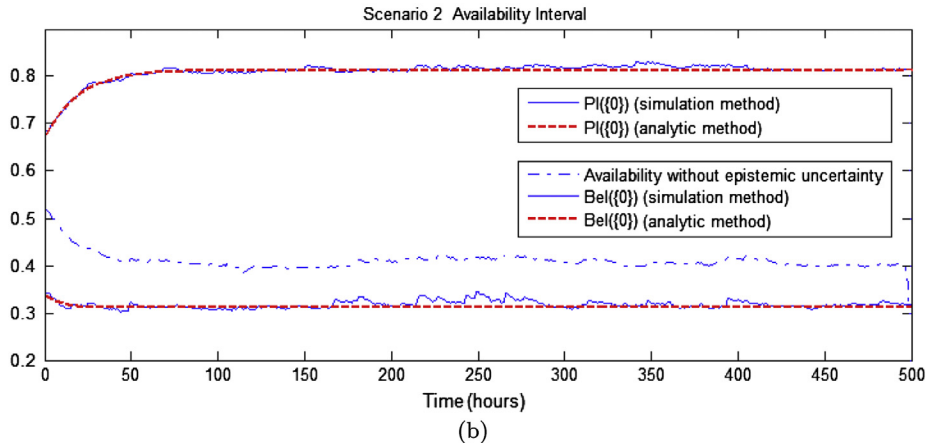
In this case, the solutions of scenario 2 are obtained as follows

$$\begin{cases} m(\{0\})(t) = a * e^{-0.06*t} + (0.0275 - a) * e^{-0.08*t} + 0.3125 \\ m(\{1\})(t) = b * e^{-0.06*t} + (0.1425 - b) * e^{-0.08*t} + 0.1875 \\ m(\mathcal{X})(t) = 0.5 - (a + b) * e^{-0.06*t} - (0.17 - a - b) * e^{-0.08*t} \end{cases} \tag{14}$$

where a and b are two unknown parameters, because the three initial conditions are not sufficient to fix the solutions.



(a)



(b)

Fig. 5. Simulation results and the analytic results of scenario 2. (a) Basic probability assignments. (b) Availability interval and the accurate availability.

We also simulate the scenario 2 in Stateflow. The simulation results and the analytic results of Eq. (14) are given in Fig. 5(a). Fig. 5(b) shows the simulation result and the analytic result of the availability interval of the binary component considering state uncertainty in scenario 2. The simulation result of the availability of the binary component without epistemic state uncertainty ($\epsilon_{0\lambda} = \epsilon_{0\mu} = \epsilon_{1\mu} = 0$) is also drawn in this figure. Obviously, the availability without epistemic state uncertainty is included in the availability interval. According to Fig. 5, the simulation result is very close to the analytic result.

From the comparison of the results of scenario 1 and scenario 2, we find that the state uncertainty in the initial conditions only influences the system availability at the beginning. It does not have any influence on the system availability after a period of time. An interesting phenomenon is that the degree of belief of the imprecision tends to be constant.

In the simulation, events in the Statechart are triggered on either of the rising edge and the falling edge of a clock. 10,000 simulations (sample time: 1 h; length of simulation: 500 h) were performed on a DELL Precision M4600 (Processor: Intel (R) Core (TM) i7-2820QM CPU @ 2.30 GHz 2.30 GHz; RAM: 8G; System type: 64-bit operating system), the whole simulation taking 1317 s. Each result curve converges to a constant after 100 h.

4. Application

In the previous section, firstly, the availability of a binary component considering state uncertainty is evaluated by an analytic method. Then, a simulation method based on the Statecharts is proposed to evaluate its availability. The simulation result is proved to be very close to the analytic result. So we can conclude that the simulation method provides the same result as the analytic method. This conclusion is very useful when systems become complex, because it is very difficult to use analytic method to evaluate the availability of complex systems.

In this section, we want to evaluate the availability of a railway signalling system considering state uncertainty. This railway signalling system is too complex to be evaluated by the analytic method, so we turn to the simulation method. This railway signalling system is ERTMS/ETCS Level 2.

4.1. ERTMS/ETCS Level 2

ERTMS is a platform supported by Europe to guarantee the interoperability across different countries and manufacturers by creating a single Europe-wide standard for train control and command systems [44]. It has two components, the first component being ETCS, which is a standard for train control systems, and the second component being GSM-R (*Global System*

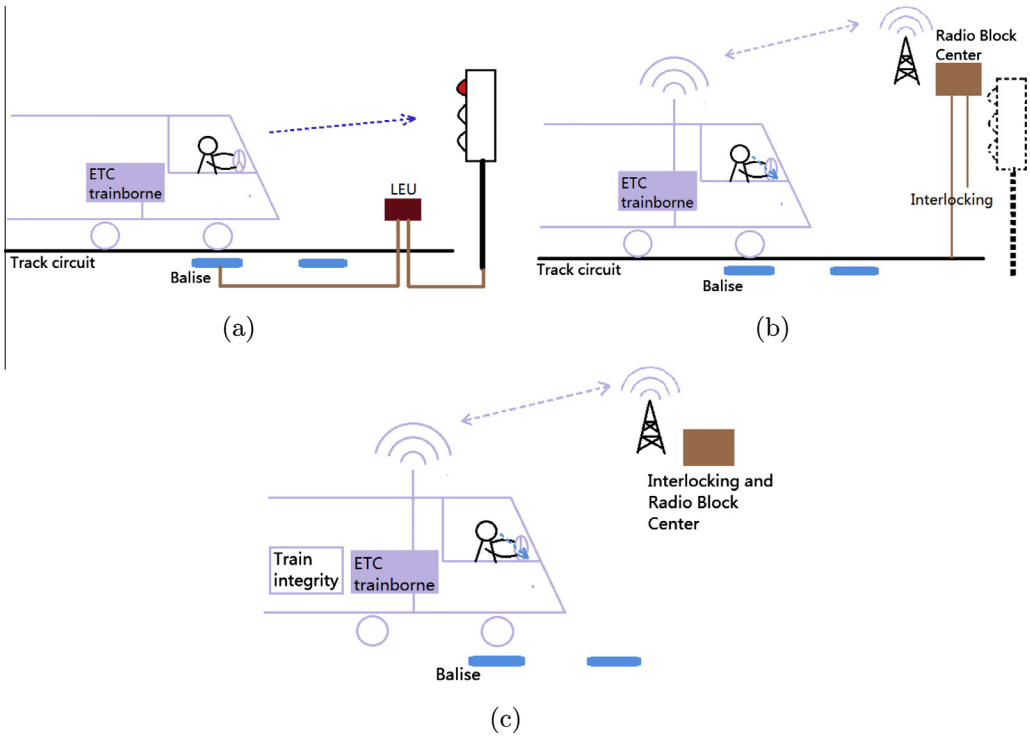


Fig. 6. Railway signalling system equipped ERTMS/ETCS. (a) Level 1. (b) Level 2. (c) Level 3.

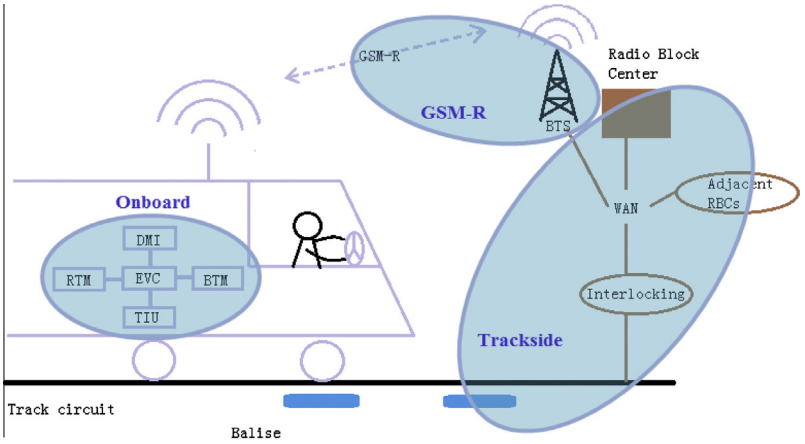
for Mobile communications – Railways), which is an international wireless communications standard for railway communication and applications.

ETCS has three levels. ETCS Level 1 and ETCS Level 2 are widely applied in Europe. ETCS Level 3 is currently under development. These different levels are distinguished by the different Trackside and Onboard ETCS equipment and different technologies of information transmission. ETCS Level 1 (Fig. 6(a)) is superimposed on the existing signalling system. The transmission of information from the track to the train-borne system is totally dependent on balises which are installed in the track. The driver controls the train according to the lineside signals. In ETCS Level 2 (Fig. 6(b)), the information transmission is by radio. The movement authority and track description are displayed directly in the cab for the driver, so lineside signals are no longer needed. Balises are used as positioning beacons to help the train to determine its position via sensors. In ETCS Level 3 (Fig. 6(c)), the train integrity checking is done by the tr ain itself, so track circuits are no longer needed. Balises are used to update position information and transmit position and integrity data back to the interlocking via GSM-R.

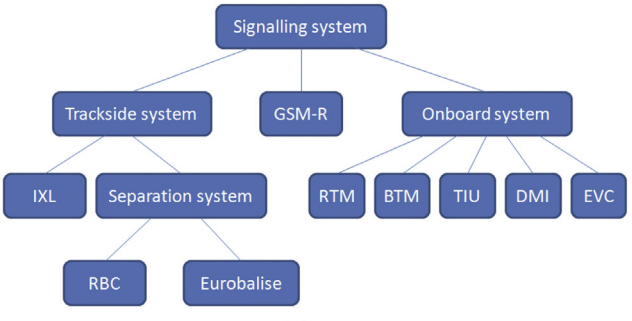
We have chosen ERTMS Level 2 as the subject of our research because it has been widely implemented in European countries, e.g., Denmark, Italy, Spain, Netherlands, France, Sweden. Fig. 7(a) describes our model of ERTMS/ETCS Level 2 inspired by the work of Flammini [45]. It consists of three parts: The Onboard system, the Trackside system and the GSM-R system. Fig. 7(b) shows its hierarchical structure.

The Onboard system receives the information coming from the Trackside system to create a "braking curve". The train driver should respect this speed profile in order to slow down or brake before stop signals or emergencies. The Onboard system also receives *telegrams* from balises and sends Position Reports (containing, for example, the train position and operating mode) to the Trackside system via GSM-R. In the Onboard system, we consider the following five modules:

- RTM (Radio Transmission Module) provides a bidirectional interface with the Trackside system via a mobile terminal.
- BTM (Balise Transmission Module) is an interface used to receive telegrams from balises and to provide power to balises.
- TIU (Train Interface Unit) provides a bidirectional interface with the train-borne equipment.
- DMI (Driver Machine Interface) provides a bidirectional interface with the train driver. It displays information and instructions to the driver, and the driver reacts to them.



(a)



(b)

Fig. 7. Railway signalling system equipped ERTMS Level 2. (a) Architecture. (b) Hierarchical structure.

- EVC (European Vital Computer) is an embedded, real-time, safety–critical computing system. It handles the telegrams from balises and measures the train speed and position in order to produce the "braking curve".

If the driver fails to perform a correct operation in time, the Onboard system will automatically call the braking procedure and begin to operate the train-borne equipment via the TIU interface.

The Trackside system performs train routing, acquires the track circuit occupation status, detects train position and sends correct speed profiles to trains. The Trackside system comprises two subsystems:

- IXL (Interlocking) is responsible for train routing and acquiring the track occupation status. It is not an object of the ERTMS standardization. It is national and different from one country to another. However, it has been stated in [44] that safety performance of the system is crucially dependent upon the integrity of the information it receives from external entities such as IXL.
- The train separation subsystem comprises Radio Block Centers (RBCs) and Eurobalises. RBCs acquire track status from linked interlocking equipment and provide trains with Movement Authorities, Static Speed Profiles and possible emergency information. Eurobalises send position telegrams to a train when the train passes over it.

GSM is a standard for mobile communications. GSM-R is an international wireless communications standard for railway communication and applications. The direction of communication is decided by the frequency of GSM-R messages. For the "Train to Track" direction the frequency of GSM-R messages is between 876 MHz and 880 MHz, whereas for the "Track to Train" direction the frequency is between 921 MHz and 925 MHz.

As a future research direction, ERTMS does not include only the components in Fig. 7(b), but the Onboard system is replicated on all the trains that are running on the line controlled by a single trackside system. This does affect availability, and the modeling of this replication is not trivial.

4.2. Modeling in Statecharts

Fig. 8(a) represents our Statechart model of the entire ERTMS/ETCS Level 2. Fig. 8(b)–(d) show the Statecharts of the three constituents of ERTMS Level 2. These Statecharts describe the communication between the Onboard system and the Trackside system via GSM-R in the presence of degradations and failures. As shown in Fig. 8(a), ERTMS/ETCS Level 2 consists of the Onboard system, the Trackside system and the GSM-R system which work in parallel.

First of all, the three systems enter the "**Waiting**" state. If the variable "Start" is true, all the systems enter the "**Normal**" state. In the "**Normal**" state, the Onboard system and the Trackside system communicate with each other via GSM-R. The Onboard system is in the "**Calculation**" state, the Trackside system is in the "**CollectionInfoCalculation**" state and the GSM-R system is in the "**CollectMessage**" state. When a *SignalFromTrack* event occurs and at the same time the frequency of GSM-R messages is not less than 900 MHz, the Trackside system sends information to the Onboard system. At this time, the Onboard system enters the "**Receive**" state, the Trackside system enters the "**Send**" state and the GSM-R system enters the "**Track2Train**" state. When an *EndSendToTrain* event occurs, the Onboard system goes back to the "**Calculation**" state, the Trackside system goes back to the "**CollectionInfoCalculation**" state and the GSM-R system goes back to the "**CollectMessage**" state. Information transmission from the Onboard system to the Trackside system functions in a similar fashion.

The Onboard system has a degraded state. When an *Operation* event occurs, if the operator is available the system enters the "**OperationByOperator**" state, and if not it enters the "**OperationByComputer**" state, which is a substate of the "**Degraded_OnBoard**" state. When *EndOperation* occurs, the system goes back to the "**Calculation**" state if the operator is unavailable, otherwise it returns to "**Normal**".

Each system has a failed state. This failed state encompasses two types of failure. The first type of failure is "**ErrorStateOfNet**". A variable "network_failed" is used to indicate the state of the whole network. The value of "network_failed" comes from statistics and once the variable is set to true, all the systems will enter the state "**ErrorState**". The failure will be repaired and systems will return to the state "**CorrectState**" when a *RepairNet* event occurs. The second type of failure is "**OrderOfErrorOfNet**". When the rail traffic controller discovers an abnormality in the network communication, he or she can give an *ErrorTrain2Track* or *ErrorTrack2Train* order immediately in order to interrupt the network and make all the systems enter the "**OrderOfErrorOfNet**" state. This type of failure can be repaired by corresponding repair events including *RepairSend_OB*, *RepairReceive_OB* and *R epairSend_TS*. It is only when both types of failure are repaired that systems can return to the "**Normal**" or "**Degraded**" state.

There is a fictive state in the Onboard system, the Trackside system and the GSM-R system. Each system has a probability to enter into the "**Uncertainty**" state and a probability to return to the "**Normal**" state. These probabilities depend on their corresponding transition rates.

When the variable "End" is true, all the systems go back to the "**Waiting**" state.

4.3. Evaluation of availability

European Economic Interest Group (EEIG) ERTMS Users Group [46] offered an ERTMS/ETCS RAMS Requirements Specification. According to this specification, the operational availability of the ERTMS/ETCS, due to all the causes of failure, shall be

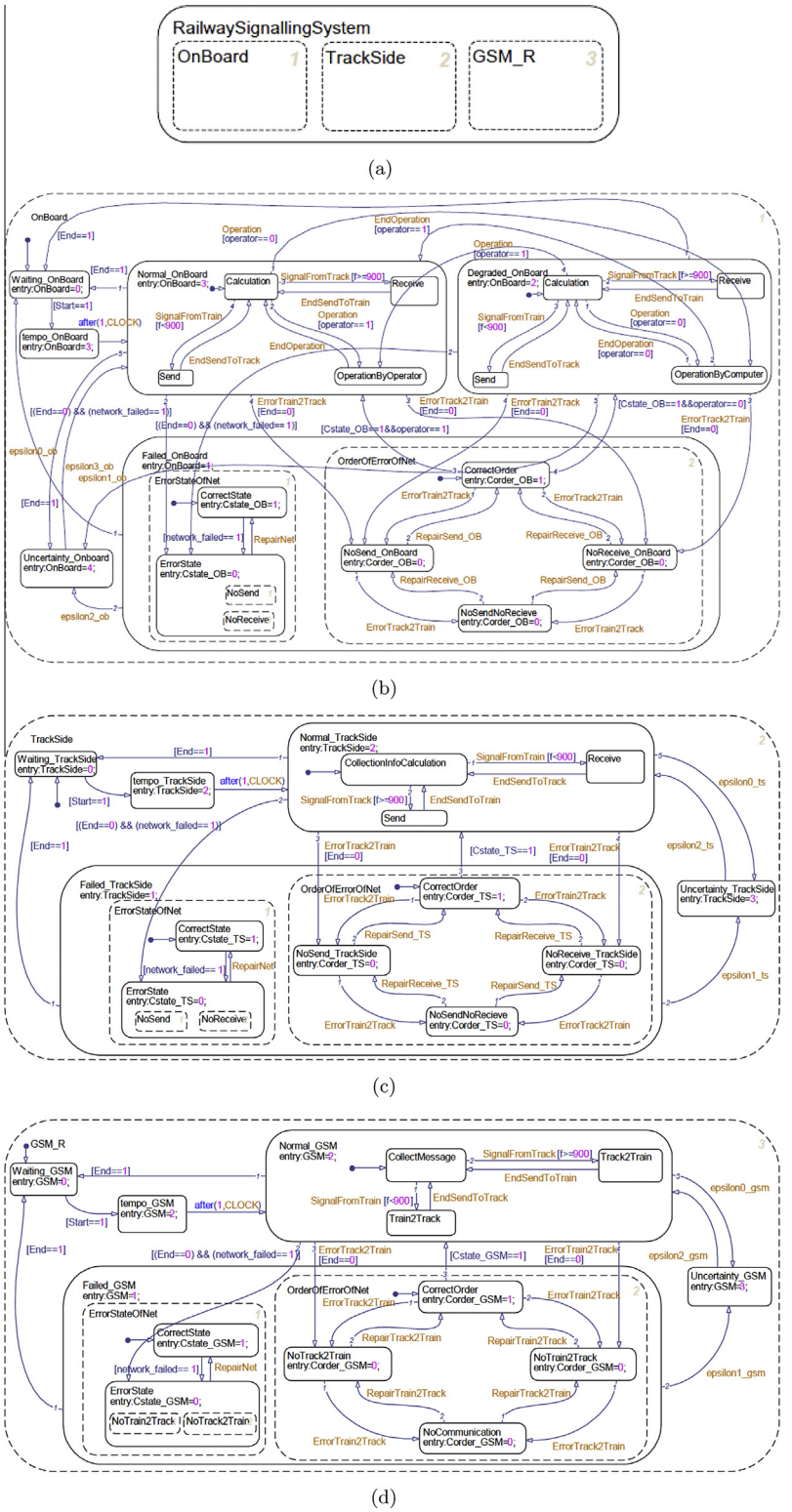


Fig. 8. Statecharts in Stateflow. (a) ERTMS/ETCS Level 2. (b) Onboard system. (c) Trackside system. (d) GSM-R system.

not less than 0.99973. The ERTMS/ETCS quantifiable contribution to operational availability, due to hardware failures and transmission errors, shall be not less than 0.99984. The Mean Time To ReStore (MTTRS) of the Onboard Equipment is

1.737 h, the MTTRS of the Trackside Centralized Equipment is 0.869 h, and the MTTRS of the Trackside Distributed Equipment is 1.737 h. For more details about other parameters, see [46].

In our model, some events and variables in the Statechart occur at a certain probability. Our simulation step is $\Delta t = 1\,h$. The list of these events and variables with their probabilities or transition rates is as follows:

- Probability (Operation, EndOperation) = 0.95
- Probability (SignalFromTrack, EndSendToTrain, SignalFromTrain, EndSendToTrack) = 0.4
- Probability ($f < 900$) = 0.5. The direction of communication is decided by the frequency of GSM-R messages. We assume that each side has the same probability of sending messages to the other side.
- Transition Rate (operator = 0) = λ_{op}, where $\lambda_{op} = 8.514 * 10^{-5}\ \mathrm{h}^{-1}$.
- Transition Rate (network_failed = 1) = λ_{n1}, where $\lambda_{n1} = 9.3885 * 10^{-6}\ \mathrm{h}^{-1}$.
- Transition Rate (RepairNet) = μ_{n1}, where $\mu_{n1} = 0.6\ \mathrm{h}^{-1}$.
- Transition Rate (ErrorTrack2Train, ErrorTrain2Track) = λ_{n2}, where $\lambda_{n2} = 0.0001\ \mathrm{h}^{-1}$.
- Transition Rate (RepairReceive_OB, RepairSend_OB, RepairReceive_TS, RepairSend_TS, RepairTrack2Train, RepairTrain2Track) = μ_{n2}, where $\mu_{n2} = 0.6\ \mathrm{h}^{-1}$.

The values of λ_{op} and λ_{n1} come from the statistics published by Federal Railroad Administration Office of Safety Analysis [18] from 2007 to 2011. The others ($\mu_{n1}, \lambda_{n2}, \mu_{n2}$, etc.) are realistic values from experts' opinions and correspond to the values generally used in the railway system. The ERTMS RAMS specification [46] indicates the upper bounds of unavailabilities of components of the OnBoard, Trakside and line systems. The values of transition rates used in this paper are realistic and satisfy the upper bounds constraints.

As for the transition rates related to the epistemic uncertainty, there is no statistics on these parameters, so we propose some realistic values for them. For the Onboard system, all the inward transition rates of the fictive state are set to be $0.0014\ \mathrm{h}^{-1}$ (This means the system enters into the fictive state once a month) and the outward transition rate of the fictive state is set to be $0.25\ \mathrm{h}^{-1}$ (This means the system will be examined 6 times a day). For the GSM-R system, all the inward transition rates of the fictive state are set to be $0.00046\ \mathrm{h}^{-1}$ (once a trimester) and the outward transition rate of the fictive state is set to be $0.25\ \mathrm{h}^{-1}$ (6 times a day). For the Trackside system, all the inward transition rates of the fictive state are set to

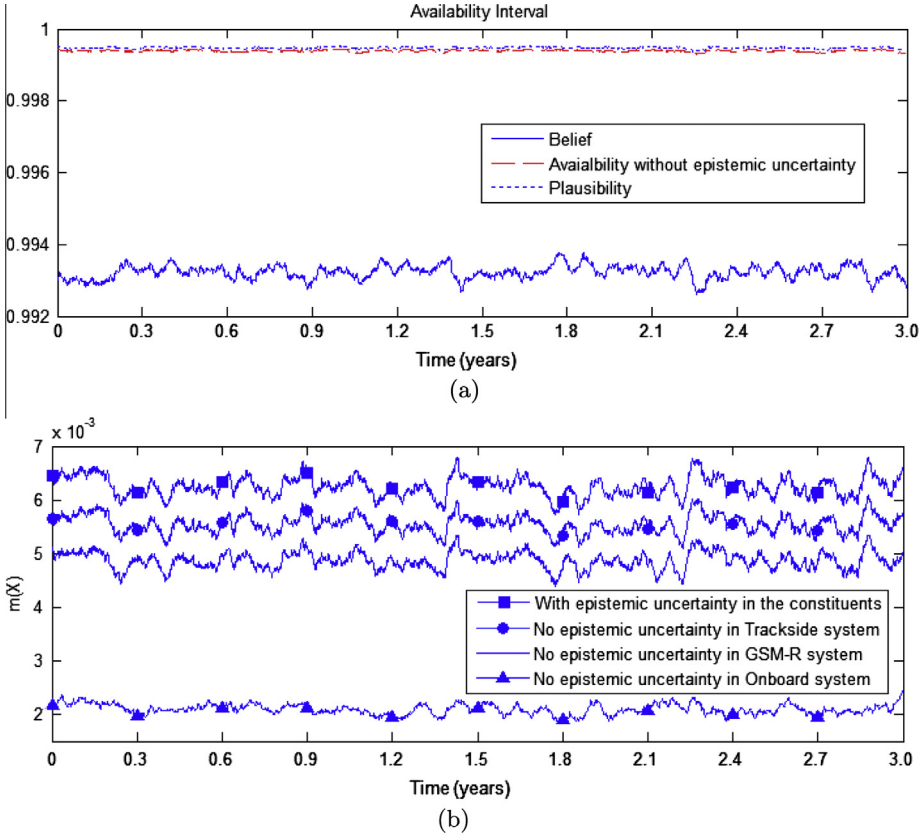


Fig. 9. Simulation results of the ERTMS/ETCS Level 2 considering state uncertainty. (a) Availability interval and the accurate availability. (b) Sensitivity analysis on the three constituent systems.

be 0.0002315 h^{-1} (once every 6 months) and the outward transition rate of the fictive state is set to be 0.25 h^{-1} (6 times a day).

Fig. 9(a) shows the simulation result of the availability interval of this signalling system during 3 years. The availability of system without epistemic uncertainty is also drawn in this figure and it is included in the availability interval. The availability without epistemic uncertainty is around 0.99949. It is a little lower than the availability given by EEIG ERTMS Users Group [46]. This result reflects the fact that some parameters in the model need more realistic values.

In the simulation, events in the Statecharts are triggered on either of the rising edge and the falling edge of a clock. 10,000 simulations (sample time: 1 h; length of simulation: 3 years) were performed on a DELL Precision M4600 (Processor: Intel (R) Core (TM) i7-2820QM CPU @ 2.30 GHz 2.30 GHz; RAM: 8G; System type: 64-bit operating system), the whole simulation taking 6.7 h. Each result curve converges to a constant after 50 h.

4.4. Sensitivity analysis

In this application, the aim of the sensitivity analysis is to estimate which constituent system's uncertainty has the most significant influence on the uncertainty of the entire ERTMS Level 2.

$m(\mathcal{X})$ represents the uncertainty of the entire ERTMS Level 2. In Fig. 9(b), the curve "With epistemic uncertainty in the constituents" shows the uncertainty of the ERTMS Level 2 with the presence of epistemic uncertainties in all the three constituent systems. The curve "No epistemic uncertainty in Trackside system" shows the uncertainty of the ERTMS Level 2 with epistemic uncertainty in Onboard system and epistemic uncertainty in GSM-R system. The curve "No epistemic uncertainty in GSM-R system" shows the uncertainty of the ERTMS Level 2 with epistemic uncertainty in Onboard system and epistemic uncertainty in Trackside system. The curve "No epistemic uncertainty in Onboard system" shows the uncertainty of the ERTMS Level 2 with epistemic uncertainty in Trackside system and epistemic uncertainty in GSM-R system. We find that the Onboard system is the system whose uncertainty influences the most significantly the uncertainty of the enti re ERTMS Level 2. The second one is the GSM-R system. The last one is the Trackside system. So if we want to reduce the uncertainty of the whole railway signalling system, we'd better begin with reducing the uncertainty in the Onboard system.

5. Conclusion

In this paper, we propose two approaches to evaluate the availability of systems considering epistemic state uncertainty: the analytic method based on the belief functions theory and the linear equations to obtain belief masses of system state, and the simulation method based on the belief functions theory and the Statecharts. We choose a discrete-time simulation with a uniform time increments Δt because it is a straightforward and easy way of modeling railway systems. However, the size of Δt can have a significant impact on the estimated availability of railway systems. The use of a discrete-event simulation or a combined discrete-time and discrete event simulation should be investigated because they can offer a fast execution and a more close result to the analytic solution.

The analytic method has been used to validate the simulation method. Compared to Statecharts in the simulation method, Markov Chain in the analytic method has two major drawbacks: inherent sequentiality and flat, non-hierarchical nature. In its classical form, the Markov Chain method is not well adapted to specify the behavior of systems because it does not support modularity and hierarchical structure. Without the concurrency and multi-level descriptions, a state-based method is not suitable to describe the behavior of large and complex systems. Furthermore, the number of states grows exponentially (we consider all possible combinations of states in all the components of the systems) in the Markov Chain method. Statecharts augmented with probabilities overcome the limitations of Markov Chain method. They support the hierarchy of states and orthogonal regions. States can be combined into a higher level state. The source state and the target state of a transition are not restr icted to the same level. These advantages make Statecharts well adapted to model large and complex systems and their dynamic behavior.

Epistemic state uncertainty is analyzed by belief functions theory. The proposed simulation method has been applied on a railway signalling system ERTMS/ETCS Level 2. We evaluated its availability when there is state uncertainty and did the sensitivity analysis to estimate the influence of uncertainties existing in the three constituent systems on the ERTMS Level 2. The proposed approach will provide a straightforward and easy method for railway community to evaluate the RAMS parameters of railway systems in presence of several type of uncertainty. Indeed, the proposed Statecharts models based are based on Discrete-events simulation and can be implemented in every simulation tool. In our future work, we plan to integrate the parametric uncertainty in some transition rates and more detailed state uncertainty into the model to enrich our uncertainty analysis.

Acknowledgments

This work was carried out and funded in the framework of the Labex MS2T. It was supported by the French Government, through the "Investments for the future" program, managed by the National Agency for Research (Reference ANR-11-IDEX-0004-02).

This work was also supported by the French National Research Agency, ANR-13-JS03-0007 RECIF.

Appendix A

A.1. Availability of a binary component without state uncertainty

According to Fig. 2(b), the availability of being in the working state and in the failed state can be calculated analytically as follows

$$\begin{cases} A_0(t+\Delta t) = A_0(t)(1-\lambda\Delta t) + A_1(t)\mu\Delta t \\ A_1(t+\Delta t) = A_1(t)(1-\mu\Delta t) + A_0(t)\lambda\Delta t \end{cases} \tag{15}$$

$$\begin{cases} \lim_{\Delta t\to 0} \frac{A_0(t+\Delta t)-A_0(t)}{\Delta t} = A_0\prime(t) = -A_0(t)\lambda + A_1(t)\mu \\ \lim_{\Delta t\to 0} \frac{A_1(t+\Delta t)-A_1(t)}{\Delta t} = A_1\prime(t) = -A_1(t)\mu + A_0(t)\lambda \end{cases} \tag{16}$$

The initial conditions are $A_0(0) = 1$ and $A_1(0) = 0$. So finally the availability of being in the working state and in the failed state is obtained as follows

$$\begin{cases} A_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \\ A_1(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \end{cases} \tag{17}$$

A.2. Availability of a binary component considering state uncertainty

According to Fig. 3(a), we have the following equations

$$\begin{cases} m(\{0\})(t+\Delta t) = m(\{0\})(t) * (1-\lambda\Delta t - \epsilon_{0\lambda}\Delta t) + m(\{1\})(t) * \mu\Delta t + m(\mathcal{X})(t) * \epsilon_{0\mu}\Delta t \\ m(\{1\})(t+\Delta t) = m(\{1\})(t) * (1-\mu\Delta t - \epsilon_{1\mu}\Delta t) + m(\{0\})(t) * \lambda\Delta t \end{cases} \tag{18}$$

where $m(\{0\})(t) + m(\{1\})(t) + m(\mathcal{X})(t) = 1$.

$$\begin{cases} m(\{0\})'(t) = m(\{0\})(t) * (-\lambda - \epsilon_{0\lambda} - \epsilon_{0\mu}) + m(\{1\})(t) * (\mu - \epsilon_{0\mu}) + \epsilon_{0\mu} \\ m(\{1\})'(t) = m(\{1\})(t) * (-\mu - \epsilon_{1\mu}) + m(\{0\})(t) * \lambda \end{cases} \tag{19}$$

To find the solutions of Eq. (19), we simplify it in the following form

$$\begin{cases} x'(t) = x(t) * a_1 + y(t) * b_1 + c_1 \\ y'(t) = x(t) * a_2 + y(t) * b_2 \end{cases} \tag{20}$$

where $x(t) = m(\{0\})(t), y(t) = m(\{1\})(t)$ and

$$\begin{cases} a_1 = -\lambda - \epsilon_{0\lambda} - \epsilon_{0\mu} \\ b_1 = \mu - \epsilon_{0\mu} \\ c_1 = \epsilon_{0\mu} \\ a_2 = \lambda \\ b_2 = -\mu - \epsilon_{1\mu} \end{cases} \tag{21}$$

From Eq. (20), we have

$$y''(t) - y'(t) * (a_1 + b_2) + y(t) * (a_1 b_2 - a_2 b_1) - a_2 c_1 = 0 \tag{22}$$

This is a Second order Linear Homogeneous Differential Equation with Constant Coefficients. The form of the final solution should be a general solution plus a particular solution. In our case, the particular solution is

$$particular\,solution = \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \tag{23}$$

The corresponding characteristic equation is

$$k^2 - k * (a_1 + b_2) + (a_1 b_2 - a_2 b_1) = 0 \tag{24}$$

The roots of the characteristic equation are

$$k_{1,2} = \frac{a_1 + b_2 \pm \sqrt{(a_1 - b_2)^2 + 4a_2 b_1}}{2} \tag{25}$$

According to the roots of the characteristic equation, there are three cases for the general solution of $y(t)$. The same with $x(t)$. Finally, we get three different cases of the solutions of $x(t)$ and $y(t)$ in the following forms

- If $(a_1 - b_2)^2 + 4a_2b_1 > 0$

$$\begin{cases} x(t) = n_1 e^{k_1 t} + n_2 e^{k_2 t} - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ y(t) = m_1 e^{k_1 t} + m_2 e^{k_2 t} + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{26}$$

- If $(a_1 - b_2)^2 + 4a_2b_1 = 0$

$$\begin{cases} x(t) = (n_1 + n_2 t) e^{k_1 t} - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ y(t) = (m_1 + m_2 t) e^{k_1 t} + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{27}$$

- If $(a_1 - b_2)^2 + 4a_2b_1 < 0$

$$\begin{cases} x(t) = e^{\alpha t}(n_1 \cos \beta t + n_2 \sin \beta t) - \frac{b_2 c_1}{a_1 b_2 - a_2 b_1} \\ y(t) = e^{\alpha t}(m_1 \cos \beta t + m_2 \sin \beta t) + \frac{a_2 c_1}{a_1 b_2 - a_2 b_1} \end{cases} \tag{28}$$

where α and β come from $k_{1,2} = \alpha \pm i * \beta$.

n_1, n_2, m_1, m_2 are unknown. Initial conditions are needed to fix their values.

References

[1] E.L. Droguett, M.D.C. Moura, C.M. Jacinto, M.F. Silva Jr., A semi-markov model with bayesian belief network based human error probability for availability assessment of downhole optical monitoring systems, Simul. Modell. Pract. Theory 16 (10) (2008) 1713–1727.
[2] J. Schryver, J. Nutaro, M. Haire, Metrics for availability analysis using a discrete event simulation method, Simul. Modell. Pract. Theory 21 (1) (2012) 114–122.
[3] H. Hermanns, D.N. Jansen, Y.S. Usenko, From StoCharts to MoDeST: a comparative reliability analysis of train radio communications, in: Proceedings of the 5th International Workshop on Software and Performance, WOSP '05, ACM Press, New York, USA, 2005, pp. 13–23.
[4] D. Vernez, F. Vuille, Method to assess and optimise dependability of complex macro-systems: application to a railway signalling system, Safety Sci. 47 (3) (2009) 382–394.
[5] J. Lalouette, R. Caron, F. Scherb, N. Brinzei, J. Aubry, O. Malassé, Performance assessment of european railway signalling system superposed of the French system in the presence of failures, in: Lamda-Mu'2010, vol. 2, La Rochelle, France, 2010, pp. 2–9.
[6] J. Beugin, J. Marais, Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization, Trans. Res. Part C: Emerging Technol. 22 (2012) 42–57.
[7] A. Herranz, G. Marpons, C. Benac, J. Marino, Mechanising the validation of ERTMS requirements and new procedures, in: 9th World Congress on Railway Research, Lille, France, 2011, p. 33.
[8] EuRailCheck. <https://es.fbk.eu/projects/eurailcheck/index.php>.
[9] S. Bernardi, F. Francesco, S. Marrone, J. Merseguer, C. Papa, V. Vittorini, Model-driven availability evaluation of railway control systems, in: 30th International Conference on Computer Safety, Reliability and Security (Safecomp'11), Napoli, Italy, 2011, pp. 15–28.
[10] F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini, Modeling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks, in: Safety and reliability for managing risk:Proceedings of the 15th European Safety and Reliability Conference(ESREL2006), Estoril, Portugal, 2006, pp. 2675–83.
[11] A. Zimmermann, G. Hommel, A train control system case study in model-based real time system design, in: Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS '03), vol. 00, no. C, IEEE Computer Society, Washington, DC, USA, 2003.
[12] R. Zhang, S. Mahadevan, Model uncertainty and Bayesian updating in reliability-based inspection, Struct. Safety 22 (2) (2000) 145–160.
[13] T. Nilsen, T. Aven, Models and model uncertainty in the context of risk analysis, Rel. Eng. Syst. Saf. 79 (3) (2003) 309–317.
[14] R.L. Winkler, Uncertainty in probabilistic risk assessment, Rel. Eng. Syst. Saf. 54 (2-3) (1996) 127–132.
[15] T. Aven, T. Nøkland, On the use of uncertainty importance measures in reliability and risk analysis, Rel. Eng. Syst. Saf. 95 (2) (2010) 127–133.
[16] T. Aven, Interpretations of alternative uncertainty representations in a reliability and risk analysis context, Rel. Eng. Syst. Saf. 96 (3) (2011) 353–360.
[17] M. Drouin, G. Parry, J. Lehner, G. Martinez-Guridi, J. LaChance, T. Wheeler, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-informed Decision making, NUREG1855, vol. 1, 2009.
[18] Federal Railroad Administration Office of Safety Analysis, Federal Railroad Administration Office of Safety Analysis, 2013. <http://safetydata.fra.dot.gov/officeofsafety/default.aspx>.
[19] D. Dubois, Representation, propagation, and decision issues in risk analysis under incomplete probabilistic information, Risk Anal. 30 (3) (2010) 361–368.
[20] D. Blockley, Analysing uncertainties: towards comparing Bayesian and interval probabilities, Mech. Syst. Signal Process. (2012) 1–13.
[21] P. Walley, Statistical Reasoning with Imprecise Probabilities, Chapman and Hall, London, 1991.
[22] S. Kikuchi, P. Chakroborty, Place of possibility theory in transportation analysis, Trans. Res. Part B: Meth. 40 (8) (2006) 595–615.
[23] D. Dubois, Possibility theory and statistical reasoning, Comput. Statist. Data Anal. 51 (1) (2006) 47–69.
[24] A.P. Dempster, Upper and lower probabilities induced by a multivalued mapping, Ann. Math. Statist. 38 (1967) 325–339.
[25] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, New Jersey, 1976.
[26] M. Guth, A probabilistic foundation for vagueness and imprecision in fault-tree analysis, IEEE Trans. Rel. 40 (5) (1991) 563–571.
[27] T. Inagaki, Interdependence between safety-control policy and multiple-sensor schemes via Dempster–Shafer theory, IEEE Trans. Rel. 40 (2) (1991) 182–188.
[28] C. Simon, P. Weber, Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge, IEEE Trans. Rel. 58 (1) (2009) 69–87.
[29] M. Sallak, W. Schön, F. Aguirre, The Transferable Belief Model for reliability analysis of systems with data uncertainties and failure dependencies, Proc. Inst. Mech. Eng. Part O: J. Risk Rel. 40 (2010) 266–278.
[30] Object Management Group, OMG Unified Modeling Language (OMG UML), Superstructure, 2011.
[31] D. Harel, Statecharts: a visual formalism for complex systems, Sci. Comput. Programming 8 (1987) 231–274.
[32] F. Cicirelli, A. Furfaro, L. Nigro, Modelling and simulation of complex manufacturing systems using statechart-based actors, Simul. Modell. Pract. Theory 19 (2) (2011) 685–703.
[33] P. Gruer, A. Koukam, B. Mazigh, Modeling and quantitative analysis of discrete event systems: a statecharts based approach, Simul. Pract. Theory 6 (4) (1998) 397–411.
[34] C.R.L. Frances, E. da Luz Oliveira, J.C.W.A. Costa, M.J. Santana, R.H.C. Santana, S.M. Bruschi, N.L. Vijaykumar, S.V. de Carvalho, Performance evaluation based on system modeling using statecharts extensions, Simul. Modell. Pract. Theory 13 (7) (2005) 584–618.

[35] A. Jaoua, D. Riopel, M. Gamache, A simulation framework for real-time fleet management in internal transport systems, Simul. Modell. Pract. Theory 21 (1) (2012) 78–90.
[36] M. Banci, A. Fantechi, S. Gnesi, The role of formal methods in developing a distribuited railway interlocking system, in: Proc. of the 5th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2004), 2004, pp. 220–230.
[37] Z. Pap, I. Majzik, A. Pataricza, A. Szegi, Methods of checking general safety criteria in UML statechart specifications, Rel. Eng. Syst. Saf. 87 (1) (2005) 89–107.
[38] J. Magott, P. Skrobanek, Timing analysis of safety properties using fault trees with time dependencies and timed state-charts, Rel. Eng. Syst. Saf. 97 (1) (2012) 14–26.
[39] Y. Liang, M.A. Smith, K.S. Trivedi, Uncertainty analysis in reliability modeling, in: Annual Reliability and Maintainability Symposium, 2001, pp. 229–234.
[40] M. Marseguerra, E. Zio, L. Podofillini, D.W. Coit, Optimal design of reliable network systems in presence of uncertainty 54(2) (2005) 243-253.
[41] A.P. Dempster, New methods for reasoning towards posterior distributions based on sample data, Ann. Math. Statist. 37 (1966) 355–364.
[42] J.C. Helto, J.D. Johnson, W.L. Oberkampf, C.B. Storlie, A Sampling-Based Computational Strategy for the Representation of Epistemic Uncertainty in Model Predictions with Evidence Theory, Sandia National Laboratories, California, Tech. Rep. October, 2006.
[43] D. Drusinsky, D. Harel, Using statecharts for hardware description and synthesis, IEEE Trans. Comput.–Aided Des. Integr. Circ. Syst. 8 (7) (1989) 798–807.
[44] UNISIG SUBSET-091 (version 3.2.0), Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, 2009.
[45] F. Flammini, Model-Based Dependability Evaluation of Complex Critical Control Systems, VDM Verlag, Germany, 2009.
[46] EEIG ERTMS Users Group, ERTMS/ETCS RAMS Requirements Specification, 1998.