Affidabilità e sicurezza dei sistemi innovativi di comando/controllo. Approcci basati su modelli e loro applicazioni industriali

Reliability, safety and security of innovative command/control systems. Model-based approaches and related industrial applications

Dott. Ingg. Francesco Flammini(*), Leonardo Impagliazzo(*), Pietro Marmo(*), Concetta Pragliola(*)

1. Introduzione

Dai primi anni 90' è in corso una transizione dei sistemi di controllo ferroviari dalle tradizionali logiche elettromeccaniche realizzate a relè verso i più moderni sistemi di elaborazione dedicati per: la gestione degli itinerari, il distanziamento treni, il controllo della marcia e la supervisione del traffico. Per tutte le funzionalità la cui disponibilità e correttezza ha notevole impatto sui costi di manutenzione con possibili ripercussioni anche sulla sicurezza, è indispensabile adottare strumenti di progetto e collaudo che seguano le direttive degli standard internazionali [1]. In tale contesto, l'impiego di modelli può avere molteplici vantaggi, in termini di supporto alle scelte progettuali fin dalle prime fasi del ciclo di sviluppo, della valutazione e dimostrazione degli indici di affidabilità e sicurezza in fase di certificazione, e finanche delle capacità diagnostica e prognostica in fase operativa. Al fine di adeguare la scelta dei formalismi all'obiettivo dell'analisi, al livello di astrazione, alla natura e alle dimensioni dei sistemi, è opportuno adottare adeguati metodi e strumenti modellistici che supportino, tra le altre cose, paradigmi di tipo modulare. In particolare, alcuni formalismi si prestano a diverse tipologie di analisi, supportando la valutazione analitica sia di attributi RAMSS[1] che di proprietà che devono essere soddisfatte dal sistema [2]. Un approccio olistico (ovvero integrato e coeso) basato su diversi formalismi consente di evitare ipotesi eccessivamente conservative che tendono inoltre a trascurare determinate dinamiche di interazione tra sottosistemi. In fase di progettazione, ciò potrebbe avere l'effetto di ottenere risultati poco attendibili o troppo conservativi, con una non ottimale allocazione degli sforzi di sviluppo tra i diversi componenti. La calibrazione fine nella scelta dei formalismi e

(*) Ansaldo STS.

(1) *Reliability Availability Maintainability Safety Security* (Affidabilità, Disponibilità, Manutenibilità, Innocuità, Protezione; questi ultimi due attributi il più delle volte tradotti nella nostra lingua con il termine "Sicurezza").

1. Introduction

Since the beginning of the 1990's, a transition of railway control systems has been in progress, from the traditional electromechanical relay logics to modern embedded computer systems for: train and route control, interlocking, traffic management, supervision and train dispatching. For all the functions in which the availability and correctness has a notable impact on maintenance costs and possibly system safety, it is necessary to adopt methods and tools that follow the prescriptions of international standards [1]. In that context, the application of models has multiple advantages, in terms of supporting design choices from the first phases of system development cycle, for the evaluation and demonstration of reliability, safety and security indices in the certification stage, and also for the diagnostic and prognostic capabilities in the operational phase. In order to tune the choice of the formalisms to the objectives of the analysis, to the level of abstraction and to the nature and size of the system, engineers need appropriate methods and modelling tools that support, among other things, modular techniques. In particular, some formalisms are suited to different types of analysis, supporting the analytic evaluation both of RAMSS[1] attributes and properties that must be fulfilled by the system [2]. A holistic (i.e. cohesive and integrated) approach based on different formalisms allows engineers to avoid conservative hypotheses that neglect certain interaction dynamics between subsystems. In the design stage, that could have the effect of obtaining imprecise or conservative results, with a sub-optimal allocation of the development efforts among the different components. In other words, the fine tuning of the formalisms and of the abstraction levels of the models allows balancing expressive power, ease of use and solving efficiency.

In this paper, the aforementioned concepts will be applied to industrial case-studies in the railway and metro-

(1) *Reliability Availability Maintainability Safety Security.*

del livello di astrazione dei modelli consente, in definitiva, di bilanciare potenza espressiva, facilità d'uso ed efficienza risolutiva.

Nel corso di questo articolo, i concetti generali precedentemente esposti verranno applicati a casi industriali nel settore del trasporto ferroviario e metropolitano. A tal scopo, ognuno dei paragrafi che seguono presenterà un'esperienza di risoluzione di una o più problematiche relative alla sicurezza o all'affidabilità dei sistemi basata su tecniche di modellazione avanzate. Tali esperienze evidenziano un efficace trasferimento in ambito industriale di metodi e strumenti sviluppati in ambito accademico. Verranno infine tratte delle conclusioni generali, discutendo i risultati ottenuti e fornendo alcune linee guida sui futuri sviluppi della ricerca accademica ed industriale.

Più in dettaglio, l'articolo è strutturato come segue:

- la seconda sezione descrive un metodo per la valutazione della disponibilità di un sistema ferroviario considerando tutte le modalità e le cause di guasto e sfruttando una tecnica di modellazione detta multi-formalismo;
- nella terza sezione viene illustrata una tecnica di valutazione della safety di sistemi di votazione a maggioranza in presenza di manutenzione imperfetta, sfruttando ancora una volta tecniche di astrazione e modellazione basata su diversi linguaggi;
- nella quarta sezione si introduce il concetto di *model-based testing* ovvero di verifiche (statiche o dinamiche) basate sul supporto di modelli, allo scopo di migliorare l'efficacia e l'efficienza del processo di certificazione;
- nella quinta sezione si presenta un possibile approccio per la valutazione del rischio *security* attraverso modelli eterogenei, trasferendo a tale ambito - ed in alcuni casi estendendo - tecniche sviluppate e tradizionalmente impiegate per le valutazioni di affidabilità e *safety*;
- infine, nella sesta sezione si mostra come modelli formali possano essere impiegati per rilevare in tempo reale minacce di diversa natura, allo scopo di realizzare un sistema di allerta precoce e supporto alle decisioni in fase operativa.

Per una trattazione teorica della modellistica dei sistemi critici, in cui vengono introdotti sia i formalismi di base che le tecniche avanzate, il lettore può far riferimento a [3]. Per alcuni elementi introduttivi sui formalismi di base si veda la tabella 1.

2. Valutazioni olistiche di disponibilità

Supponiamo di avere la necessità di valutare la disponibilità di un complesso sistema di controllo ferroviario. Innanzitutto, tale valutazione richiede in via preliminare di definire con precisione qual è la modalità di fallimento a cui ci si riferisce. Nel caso dello standard ERTMS/ETCS (*European Railway Traffic Management System/European Train Control System* [4]), impiegato su tutte le nuove linee ad Alta Velocità/Alta Capacità (AV/AC), vengono definiti i seguenti tre modi di fallimento:

politan transport sectors. To this aim, each of the following sections will present an application of advanced modelling techniques to problems related to safety, reliability and security. Those experiences highlight an efficient transfer to the industry of tools and methods developed in the academy. Finally, general conclusions will be drawn by discussing the obtained results and providing some pointers to future academic and industrial research.

The rest of this article is structured as follows:

- the second section describes a method for the availability evaluation of a railway system considering all the failure modes and fault origins and exploiting a modelling technique known as "multi-formalism";
- in the third section we illustrate a safety evaluation technique for majority voting systems in presence of imperfect maintenance, using abstraction and modelling techniques based on different languages;
- in the fourth section the concept of *model-based-testing* – that is (static or dynamic) verifications based on the support of models – is introduced, with the aim of improving effectiveness and efficiency of the certification process;
- in the fifth section a possible approach for the *security* risk evaluation through heterogeneous models is presented, which transfers to that field – and in certain cases extends – techniques developed and traditionally employed for the evaluation of reliability and safety;
- finally, in the sixth section we show how formal models can be employed for the real-time detection of threats of different nature, with the aim of developing an early warning and decision support tool to be used in the operational phase.

For a theoretical introduction of critical systems modelling, in which both basic formalisms and advanced techniques are described, the reader may refer to [3]. For some introductive elements on basic formalisms see table 1.

2. Holistic availability evaluation

Let us assume we need to evaluate the availability of a complex railway control system. First of all, such an evaluation requires us to precisely define which failure modes we refer to. In case of the ERTMS/ETCS (*European Railway Traffic Management System/European Train Control System* [4]) standard, employed on all the new High Speed/High Capacity lines, the following three types of failure are defined:

- immobilising failure (at least 2 trains are obliged to move in an on-sight mode);
- service failure (at most one train is obliged to move in an on-sight mode);
- minor failure (requiring an unscheduled maintenance intervention, but not included in the previous categories).

TABELLA – *TABLE 1*

ALCUNI FORMALISMI ADATTI AD ANALISI DI AFFIDABILITÀ E SICUREZZA
FORMALISMS USED FOR RELIABILITY, SAFETY AND SECURITY EVALUATION

Alberi dei Guasti - *Fault Trees*
Gli alberi dei guasti sono un formalismo tradizionalmente impiegato in analisi probabilistiche del rischio. Essi mettono in relazione un evento indesiderato (detto *Top Event*), tipicamente un malfunzionamento, con una serie di eventi base (detti *Basic Event*) secondo una struttura grafica ad albero binario, in cui il *Top Event* rappresenta la radice ed i *Basic Event* le foglie. Tutti gli eventi sono connessi tra loro secondo gli operatori classici della logica booleana (*AND*, *OR*) ed eventuali altri connettori ad hoc introdotti nelle varie estensioni del formalismo proposte in letteratura (alberi dei guasti dinamici, parametrici, riparabili, ecc.). Efficienti da risolvere attraverso approcci combinatori basati sui cosiddetti "insiemi di taglio minimi", sono caratterizzati da una potenza espressiva ridotta (ad es. non possono modellare politiche di manutenzione diverse dalla "riparazione perfetta").
*The Fault Trees are a formalism traditionally employed in probabilistic risk analyses. They relate the occurrence of an undesired event (*Top Event*), typically a system failure, to a set of elementary events (*Basic Event*) according to a binary tree structure, in which the* Top Event *represents the root and the* Basic Events *the leaves. All the events are connected to each other using the classical operators of the Boolean logic (AND, OR) and other possible ad-hoc connectors introduced in the various extensions of formalism proposed in the scientific literature (Dynamic, Parametric, Repairable, etc.). They are efficiently solved through combinatory approaches based on the so called "minimal cut sets"; however, they feature a limited expressive power (for example, they cannot model maintenance policies differing from the "perfect repair").*

Automi a stati finiti - *Finite State Automata*
Gli automi o macchine a stati finiti sono un formalismo basato sui concetti di stato e transizione tra stati. Il sistema modellato evolve nel tempo in funzione dello stato attuale e dell'input ricevuto. Gli automi possono modellare in modo più o meno astratto un gran numero di sistemi dinamici. Ne esistono numerose estensioni (tra cui automi non deterministici, ibridi, temporizzati, ecc.), che si prestano in particolare alla verifica di proprietà attraverso tecniche di *model checking*.
The Finite State Automata (or Machines) are a formalism based on the concepts of states and transitions (between states). The modelled system evolves over time as a function of the current state and of the received input. The automata can model a large number of dynamic systems in a more or less abstract manner. There exist numerous extensions (including non deterministic, hybrid, timed, etc.), which are suitable for the automatic verification of properties through model-checking *techniques.*

Catene di Markov - *Markov Chains*
Una catena di Markov a tempo continuo rappresenta graficamente un processo stocastico discreto in cui i nodi individuano stati e gli archi transizioni tra stati, a cui sono associate distribuzioni di probabilità di tipo esponenziale (che soddisfano la proprietà di "assenza di memoria"). Date le proprietà del processo, il comportamento del sistema modellato al tempo t dipende solo dallo stato in cui il sistema si trova e non da quelli precedentemente attraversati. L'utilizzo di tale formalismo è molto diffuso nelle analisi di manutenibilità.
Continuous Time Markov Chains represent a discrete stochastic process through a graph in which the places indicate states and the arcs indicate transitions between states, which are associated exponential probability distributions (satisfying the so called "memoryless" property). Given the process properties, the behaviour of the modelled system at time t only depends on the current state and not on the past ones. The use of this formalism is widespread in maintainability analyses.

Reti di Bayes - *Bayesian Networks*
Una rete bayesiana è un grafo aciclico orientato in cui i nodi rappresentano variabili aleatorie e gli archi rappresentano le relazioni di dipendenza statistica tra le variabili, quantificate da probabilità condizionali. E' possibile dimostrare che una rete bayesiana rappresenta la distribuzione della probabilità congiunta dell'insieme di variabili rappresentate dai nodi. Tradizionalmente impiegate in applicazioni di intelligenza artificiale, negli ultimi anni le reti bayesiane hanno trovato spazio nella valutazione di affidabilità, in particolare potendo esprimere ed estendere tutto ciò che può essere rappresentato attraverso un albero dei guasti, senza ricorrere ad approcci basati sull'analisi dello spazio di stato. Le estensioni decisionali possono modellare problemi di analisi costi/benefici, mentre quelle dinamiche introducono il concetto di "tempo".
A Bayesian Network is a direct acyclic graph in which the places represent stochastic variables and the arcs represent the relationships of statistical dependence between the variables, quantified by conditional probabilities. It is possible to de-

(continua)

monstrate that a Bayesian Network represents the joined probability distribution of the set of variables represented by the places. Traditionally employed in artificial intelligence applications, in recent years Bayesian networks have found a place in the evaluation of reliability, in particular being able to express and extend the Fault Tree formalism, without resorting to approaches based on the state space analysis. The decision making extensions can model problems of cost/benefit analysis, while the dynamic extensions introduce the concept of "time".

Reti Neurali - *Neural Networks*
Le reti neurali artificiali sono modelli matematici che rappresentano l'interconnessione tra elementi definiti "neuroni artificiali", ossia costrutti matematici che in qualche misura imitano le proprietà dei neuroni viventi. Possono essere utilizzate per risolvere problemi ingegneristici di intelligenza artificiale in diversi ambiti tecnologici. In particolare, nell'ambito dell'ingegneria dell'affidabilità, esse possono essere impiegate per realizzare sistemi di diagnostica, prognostica, allerta precoce e supporto alle decisioni.
The Artificial Neural Networks are mathematical models that represent the interconnection of elements, namely "artificial neurons", which are mathematical functions which in some manner mimic the properties of actual neurons. They can be used to solve engineering problems of artificial intelligence in several technological fields. In particular, in the reliability engineering field they can be employed in order to develop diagnostic, prognostic, early warning and decision support systems.

Reti di Petri - *Petri Nets*
Una rete di Petri è una rappresentazione matematica di un sistema distribuito discreto. Essa è caratterizzata da nodi *posti*, nodi *transizioni* e archi orientati che connettono posti e transizioni. Nei posti possono essere contenuti dei *token* (letteralmente "gettoni"), che possono abilitare lo scatto delle transizioni secondo opportune regole. A seguito dello scatto delle transizioni, uno o più gettoni vengono consumati dai posti di *input* ed eventuali altri vengono generati in quelli di *output*. Estese con priorità, archi multipli ed archi inibitori, le reti di Petri hanno la stessa potenza espressiva della macchina di Turing, ovvero virtualmente illimitata. Di uso non immediato, le reti di Petri "base" si prestano ad analisi di proprietà strutturali (es. assenza di *deadlock*, ovvero "stalli"), mentre le estensioni cosiddette temporizzate e/o stocastiche consentono analisi anche di tipo quantitativo (es. indici di prestazioni e/o affidabilità).
A Petri Net is a mathematical representation of a discrete distributed system. Its elements are places, transitions and directed arcs connecting places and transitions. In the places there can be tokens, which can enable the shooting of the transitions according to appropriate rules. Following the shooting of the transition, one or more tokens are removed by the input places and others are generated in the output places. If extended with priority, multiple and inhibitor arcs, Petri Nets have the same expressive power of Turing machines, that is virtually unlimited. Petri Nets are not straightforward to use. The basic formalism allows structural property analyses (e.g. absence of deadlocks), while its timed and/or stochastic extensions also enable quantitative analyses (e.g. computation of reliability and performance indices).

- guasto immobilizzante (almeno due treni sono costretti a muoversi in modalità degradata "a vista");
- guasto di servizio (al più un treno è costretto a muoversi in modalità degradata "a vista");
- guasto minore (ovvero che richiede un intervento di manutenzione non programmato ma non rientra nelle precedenti categorie).

A partire da ciascun modo di fallimento, l'approccio all'analisi di affidabilità tradizionale attraverso il semplice formalismo degli alberi dei guasti (*Fault Tree*, FT) ha l'obiettivo di definire la combinazione di eventi che possono portare al fallimento. L'analisi arriva a considerare eventi base non ulteriormente scomponibili in eventi più semplici (le cosiddette "foglie") e la relativa distribuzione di probabilità. La valutazione del modello attraverso algoritmi di tipo combinatoriale consente di valutare il tasso di occorrenza del fallimento in funzione di quello degli eventi base. Gli alberi dei guasti possono parimenti modellare aspetti di disponibilità in ipotesi molto semplificative (includendo "risorse di riparazione illimitate"). Data la loro scarsa espressività, non possono modellare aspetti avanzati, come modi comuni di guasto, politiche complesse di riparazione includendo manutenzione preventiva, e guasti dovuti a degradazioni delle prestazioni o alla congestione dei canali di comunicazione (i cosiddetti aspetti di *performability*). Il formalismo delle *Catene di Markov*, invece, molto diffuso per la modellazione di sistemi riparabili, non è adatto a modellare

Starting from each failure mode, the traditional approach to reliability analyses through the simple formalism of the *Fault Trees* (FT) has the objective of defining the combination of events that could generate a failure. The analysis aims at finding events which are no further decomposable into simpler events (the so called "leaves") and the related probability distributions. The evaluation of the model through combinatorial algorithms allows to estimate system failure rate starting from the basic fault events. Similarly, fault trees can model availability aspects in very simplified and often unrealistic assumptions (including "unlimited repair resources"). Given their low expressive power, they cannot model advanced aspects, like common modes of failures, complex repair policies including preventive maintenance, and failures due to performance degradations or to the congestion of the communications channels (the so called *performability* aspects). On the other hand, the *Markov Chains* formalism, widespread for repairable systems modeling, is not suited to model

ficate ed il più delle volte poco realistiche (tra cui risorse di riparazione infinite). Data la ridotta potenza espressiva, tramite gli alberi dei guasti non risulta possibile modellare aspetti più avanzati, quali modi di guasto comune, politiche di manutenzione articolate che prevedono manutenzione preventiva, e fallimenti dovuti a cali di prestazioni dovuti alla qualità del segnale o alla congestione nei canali di comunicazione (aspetti cosiddetti di *performability*). D'altra parte, il formalismo delle catene di Markov, anch'esso diffuso per la modellazione dei sistemi riparabili, risulta poco adatto a modellare sistemi complessi con un elevato numero di stati.

Una possibile soluzione al problema consiste nel combinare più formalismi di modellazione in dipendenza degli aspetti da modellare, secondo un approccio cosiddetto "multi-formalismo" [5]. Secondo tale approccio, gli alberi dei guasti possono continuare ad essere utilizzati per modellare sotto-sistemi non riparabili on-line (ad esempio quelli di bordo treno, *on-board*), che non presentano guasti di modo comune significativi e sono caratterizzati da un unico modo di fallimento di interesse per l'analisi. Viceversa, sistemi che non presentano tali caratteristiche possono essere modellati utilizzando:

- reti di Bayes (*Bayesian Networks*, BN), che consentono di rappresentare in un unico nodo più modi di guasto e di esplicitare interdipendenze tra gli eventi. In [6] tale formalismo viene utilizzato per modellare il modello globale, rappresentando in un unico modello tutte e tre le modalità di guasto di sistema sopra elencate;
- alberi dei guasti riparabili[2] (*Repairable Fault Trees*, RFT), che consentono di modellare politiche di manutenzione articolate in qualsivoglia modo, quali manutenzione preventiva, priorità di intervento, risorse di riparazione non infinite, ecc. In [7] tale formalismo viene applicato al *Radio Block Center* (RBC), che è un sottosistema di terra (*trackside*) di ERMS/ETCS responsabile del distanziamento treni.
- reti di Petri stocastiche generalizzate (*Generalized Stochastic Petri Nets*, GSPN), adatte a modellare sia prestazioni che errori sui canali di comunicazione (e quindi l'impatto di questi ultimi sulle prestazioni) [8].

La formulazione di un modello olistico dell'intero sistema richiede la combinazione dei sottomodelli eterogenei tramite opportuni operatori di composizione. In [6], i modelli interagiscono tra loro scambiandosi dei risultati (ad es. il risultato della valutazione di un modello viene utilizzato come parametro per popolarne un altro), per cui la composizione può essere realizzata semplicemente attraverso dei cosiddetti "connettori"; in altri casi, la composizione può ricomplex systems with a high number of states.

A possible solution to the problem is to combine more modelling formalisms as a function of the aspects to be modelled, using the so called *multi-formalism* approach [5]. According to that approach, the fault trees could be used for the modelling of not on-line repairable sub-systems (for example those *on-board*), featuring no common mode of failures and a single failure mode of interest for the analyses. (Sub)Systems not featuring such characteristics can be modelled using:

- *Bayesian Networks* (BN), allowing the representation in a single node of more failure modes and to express interdependencies among events. In [6] this formalism is used for the global model, representing all the aforementioned failure modes in a single model;
- *Repairable Fault Trees*[2] (RFT), allowing the modelling of any articulated maintenance policies, including preventative maintenance, priority of intervention, limited repair resources, etc. In [7] the RFT formalism is applied to the *Radio Block Centre* (RBC), that it is a ERMS/ETCS *trackside* subsystem which is responsible for the train distancing;
- *Generalised Stochastic Petri Nets* (GSPN), suited to model both performance and transmission errors on communication channels (and therefore the impact of these errors on performance) [8].

The construction of a holistic model of the entire system requires the combination of heterogeneous sub models through appropriate composition operators. In [6], the models interact by exchanging results (for example the evaluation result of a model is used as a parameter in order to populate another model), hence the composition can be produced through the so called "connectors"; in other cases, the composition can relate to the sharing of states, events or actions.

In fig. 1 an example of a multi-formalism model of availability is shown (in which the connectors are omitted) for the ERTMS/ETCS system. In the case study, 4 different formalisms were employed (BN, FT, RFT, GSPN), according to the criteria described above. The model was used in order to evaluate the performance of Italian high-speed railways supplied by Ansaldo STS.

In summary, the multi-formalism approach enables a more detailed and manageable representation of the system, with the advantage of estimating (through parametric sensitivity analyses) the system level impact of reliability and fault-tolerance parameters, and consequently of fine tuning design choices according to their cost-effectiveness.

[2] Dal punto di vista grafico, i RFT sono delle estensioni degli alberi dei guasti tradizionali con blocchi di riparazione. Vengono risolti trasformando il modello in una corrispondente GSPN utilizzando diverse tecniche di risoluzione.

[2] From a graphical point of view, RFTs are extensions of the traditional fault trees with reparation blocks. They are solved by transforming the model into a GSPN and by using several solution techniques.

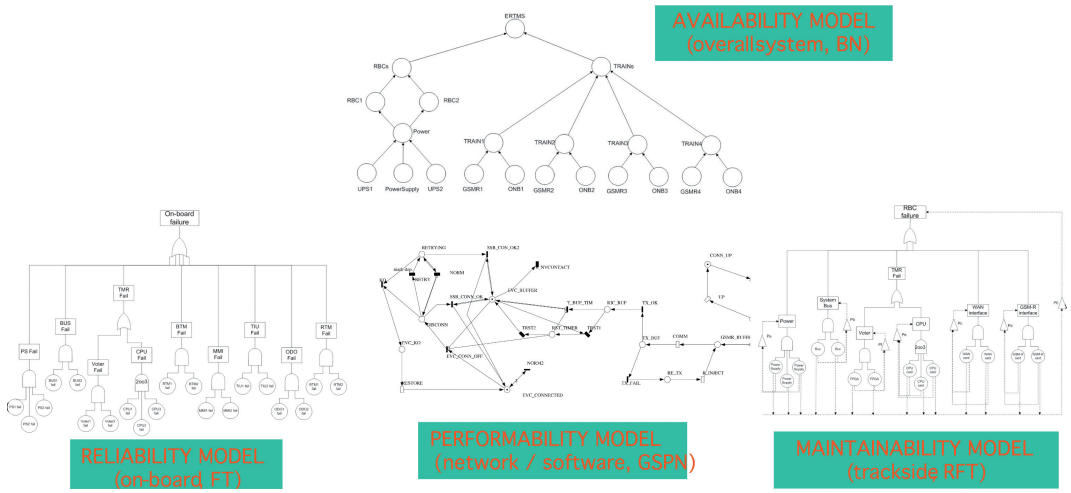

Fig. 1 - Un modello multi-formalismo di disponibilità. *A multi-formalism availability model.*

guardare la condivisione di stati, eventi o azioni.

In fig. 1 è riportata una vista di esempio relativa ad un modello multi-formalismo di disponibilità (in cui è omessa l'esplicitazione dei connettori) per il sistema ERTMS/ETCS. Nel caso di studio, sono stati impiegati quattro diversi formalismi (BN, FT, RFT, GSPN), secondo i criteri precedentemente esposti. Il modello è stato utilizzato per valutare le prestazioni delle linee ERTMS-AV Italia di fornitura ASTS.

In sintesi, l'approccio multi-formalismo rende possibile una rappresentazione più dettagliata del sistema senza rendere ingestibile il modello globale, con il vantaggio di poter stimare in modo fine (tramite opportune analisi di sensitività parametrica) l'impatto a livello di sistema di parametri di affidabilità e tolleranza ai guasti, e di calibrare di conseguenza le scelte progettuali in un'ottica di ottimizzazione costi/benefici.

3. Valutazioni di safety in presenza di manutenzione imperfetta

Molti sistemi di controllo impiegati in ambiti *safety-critical* sono basati su elaboratori *fault-tolerant* a ridondanza tripla modulare (*Triple Modular Redundancy*, TMR). L'architettura TMR consente una votazione a maggioranza "*2 out of 3*" (concordanza su almeno due sezioni) sulle uscite di tre sezioni indipendenti, isolate galvanicamente e diversamente sviluppate. In caso di malfunzionamento di una sezione, questa viene esclusa ed il sistema continua a funzionare in modalità "*2 out of 2*" (concordanza su entrambe le sezioni).

3. Safety evaluation in presence of imperfect maintenance

Many control systems employed in *safety-critical* applications are based on *fault-tolerant* processors in *Triple Modular Redundancy* (TMR) architectures. The TMR architecture allows a "2 *out of* 3" majority voting on the outputs of three independent, galvanically insulated and diversely developed sections. In case of failures in one section, this is excluded and the system continues to work in a "2 *out of* 2" configuration.

In order to evaluate the safety of TMR systems, it is possible to employ GSPN models, which take into account, among other things, the fault type (transient or permanent) and the efficiency of the self-diagnostic mechanisms [9]. GSPNs feature a very high expressive power, however they are extremely difficult to maintain. Among their defects we can list the difficult readability, the limited solving efficiency, and the support tools which are too few and hard to use. As a consequence, extensions of the models which account for further aspects, for example the ones of imperfect maintenance, are very difficult to obtain.

In order to overcome these limitations, the compromise of adopting reduced expressive power formalisms could be acceptable. One of these formalisms is the Bayesian Network [6]. The use of such a formalism, which is not based on state-space analyses, obliges the modeller to make conservative assumptions on fault latencies, but that does not create problems as long as one is able to show that the system fulfils the requirements defined by the specifications.

Per valutare la sicurezza (*safety*) di tale sistema, è possibile impiegare modelli GSPN, che tengano conto, tra le altre cose, della natura dei guasti (transitori o permanenti) e dell'efficacia dei meccanismi di auto-diagnostica [9]. A fronte di una potenza espressiva molto elevata, però, i modelli GSPN risultano poco manutenibili. Tra i loro difetti rientrano la non facile leggibilità, la limitata efficienza di risoluzione, gli strumenti di supporto che sono pochi e di uso non semplice. Di conseguenza, l'estensione dei modelli per considerare ulteriori aspetti, quale ad esempio quello della manutenzione imperfetta, risulta molto difficile.

Per ovviare a tali limitazioni, può essere accettabile il compromesso di adottare formalismi di potenza espressiva anche più ridotta. Uno dei formalismi impiegabili a tal scopo è quello delle reti di Bayes [6]. L'impiego di formalismi non basati sull'analisi dello spazio di stato obbliga ad effettuare ipotesi conservative sulla latenza dei guasti, ma ciò non crea problemi fintanto che si riesce a dimostrare che il sistema soddisfa il valore obiettivo imposto dalla specifica.

Quando la modellazione a stati risulta preferibile o irrinunciabile, è possibile combinare modelli espressi in diversi formalismi. Ad esempio, nel caso si abbia la necessità di modellare problematiche di manutenzione imperfetta, è opportuno tenere traccia dello stato del sistema per la possibilità di avere errori latenti dovuti a guasti permanenti non diagnosticabili. In tal caso, è possibile separare il modello di guasto (espresso nel formalismo più conveniente allo scopo) da quello di manutenibilità, che può essere espresso tramite macchine a stati a diversi livelli di astrazione, a seconda del dettaglio richiesto all'analisi, come rappresentato schematicamente in fig. 2 (in cui le "miniature" dei modelli nei riquadri hanno il solo scopo di dare un'idea della diversa complessità). Quest'ultimo aspetto è ancora una volta legato al risultato della valutazione nel caso di modelli di *safety*, giacché modelli più astratti hanno un numero di stati più ridotto e sono tipicamente più leggibili e quindi manutenibili, ma d'altra parte costringono il modellista ad ulteriori approssimazioni per garantire che il risultato ottenuto sia più conservativo di quello esatto.

Un'esperienza di applicazione di approcci multi-formalismo alle valutazioni di *safety* è documentata in [10]. L'applicazione è quella dei sistemi a votazione "2 out of 2" e "2 out of 3" utilizzati da Ansaldo STS per i nuclei vitali dei sistemi di controllo e segnalamento, tra cui quelli di gestione della via o *interlocking* (ACS e NVP, *encoder*, ecc.), attualmente operativi in numerose installazioni sia in Italia che all'estero. In particolare, tale lavoro dimostra la realizzabilità pratica di tali approcci in contesti industriali, descrivendo la soluzione di un problema reale, quello della valutazione dell'impatto della manutenzione imperfetta sul tempo medio tra i guasti pericolosi, difficilmente risolvibile attraverso tecniche tradizionali.

When state-based modelling is preferable or essential, it is possible to combine models expressed in different formalisms. For example, in case of imperfect maintenance problems, it is appropriate to keep track of system state since it is possible to have non diagnosable latent errors due to permanent faults. In that case, it is possible to separate the failure model (expressed in the most convenient formalism) from the maintainability model, that can be expressed through state-machines at different levels of abstraction, according to the detail requested by the analyses, as it is schematically represented in fig. 2 (in which the model "thumbnails" have the only aim of giving an idea of the different complexities). The latter aspect is linked to the evaluation result in case of the *safety* models, since more abstract models have a reduced number of states and they are typically more readable and therefore easily maintainable, but on the other hand they force the modeller into further approximations in order to guarantee that the obtained results are more conservative than the exact ones.

An example of a multi-formalism approach applied to the evaluation of *safety* is documented in [10]. The application addresses majority voting systems ("2 out of 2" and "2 out of 3") used by Ansaldo STS for the vital cores of control and signalling systems, including the ones used for route management or *interlocking* (ACS and NVP, *encoders*, etc.), which are currently operational in many installations in several countries. In particular, the referenced work shows the industrial feasibility of such an approach, describing the solution of a real problem, that is the evaluation of the impact of imperfect maintenance on the mean times between hazardous failures, which is hard to solve using traditional techniques.

4. Support to system functional verifications

In a complex system composed of different interacting subsystems, the *black-box* functional verification of the system is a delicate safety-related activity which is very difficult to manage by traditional techniques because of the high number of tests to be specified and executed. Therefore techniques allowing an optimal calibration of test-suite effectiveness and efficiency are necessary. The concept of "effectiveness" relates to the coverage of all significant conditions, both in nominal and degraded operating modes; the "efficiency" concept assures the feasibility of the verifications with reasonable resources and time efforts. To that aim, possibly automatic static and dynamic model-based techniques have been proposed in literature as a support to the verification activities.

With regards to static verifications, views derived from the *Unified Modelling Language* (UML), e.g. class and sequence diagrams, produced from the code analyses, allow performing checks against higher level specifications, according to a *bottom-up* approach borrowed from *reverse engineering* [11]. This process is outlined in

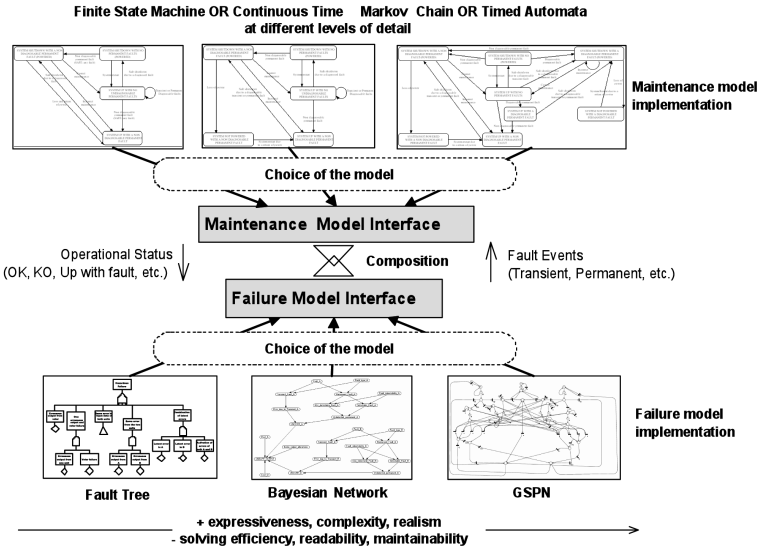

Fig. 2 - Scelta e composizione di modelli di guasto e modelli di riparazione. *Choice and composition of failure and maintenance models.*

4. Supporto alle verifiche funzionali di sistema

In un sistema complesso composto da diversi sottosistemi interagenti in vario modo tra loro, la verifica funzionale *black-box* del sistema è un'attività delicata e di fondamentale importanza per la sicurezza ma molto difficile da gestire con le tecniche tradizionali per l'elevato numero di test che sarebbe necessario effettuare. Pertanto sono necessarie tecniche che consentano di calibrare l'efficacia e l'efficienza dei casi di test al fine di raggiungere un compromesso ottimale. Il concetto di efficacia è relativo alla copertura di tutte le condizioni significative, sia nel funzionamento nominale che in quello degradato; l'efficienza assicura la fattibilità delle verifiche in tempi ragionevoli. A tal scopo, a supporto delle attività di verifica, sono state proposte in letteratura tecniche (eventualmente automatiche) statiche o dinamiche, basate su modelli di riferimento.

A livello di verifiche statiche, viste derivate dallo *Unified Modeling Language* (UML), come ad es. diagrammi delle classi e di sequenza, prodotte dall'analisi del codice, consentono di effettuare dei controlli nei confronti delle specifiche di più alto livello secondo un approccio *bottom-up* mutuato dal *reverse engineering* [11]. Il processo è schematizzato in fig. 3a. Come effetto collaterale, un'analisi di questo tipo consente di apportare delle modifiche per migliorare affidabilità e prestazioni del codice senza alterarne le funzionalità (approccio noto come *refactoring*), nel rispetto dell'indipendenza tra chi sviluppa e chi verifica come richiesto dagli standard di riferimento. Tale approccio è stato impiegato da Ansaldo STS nella fase di certificazione del sottosistema RBC di ERTMS/ETCS, a partire fig. 3a. Such an analysis allows modifications aimed at improving code reliability and performance without changing functionalities (an approach know as *refactoring*), also in the respect of the independence among development and verification teams requested by the reference standards. This approach has been employed by Ansaldo STS in the certification phase of the ERTMS/ETCS RBC subsystem, starting from the Turin-Novara high-speed system installation.

With regards to dynamic verifications, structural models can help in understanding the internal architecture of the system, in order to avoid producing all the possible combinations of the test variables. That task requires the monitoring of internal variables of the system; this aspect, together with the code coverage checks, makes such approaches not exactly "black box" but rather "grey box". The first application to SCMT ("Sistema Controllo Marcia Treni", the Italian for "Train Movement Control System") is described in [12], while a subsequent extension with the aim of automatically customizing abstract tests on real installations for computer-based interlocking systems is described in [13]. Behavioural models based on abstract finite state machines assist the engineers in deciding the minimum paths covering all the significant combinations of state and input variables (fig. 3b) [13]. This approach has been employed in system functional verifications for all the new ERTMS/ETCS systems, starting from the Rome-Naples line.

What we obtain is a procedure of *hybrid testing*, which enables several automatisms as well as the verification of the requirements for coherence, and in which the models (mainly semi-formal) play an essential role. In other words, model-based verifications allow to detect more defects in less time, speed-up corrective actions and automate the generation of test cases.

5. Security risk analyses

The terrorist attacks against railway and subway infrastructures which have happened in recent years have highlighted the issue of system protection against malicious threats. Besides terrorism, security concerns often include also natural events and vandalism; the latter can cause relevant damages to infrastructure operators.

In such a context, it is very important to be able to

dall'impianto AV Torino-Novara.

A livello di verifiche dinamiche, modelli strutturali possono aiutare nel comprendere l'architettura interna del sistema, in modo da evitare di produrre tutte le combinazioni possibili delle variabili in gioco. Ciò richiede di monitorare variabili interne al sistema, fatto che, unito alle verifiche di copertura del codice, fa sì che gli approcci di questo tipo non siano completamente "a scatola nera", ma piuttosto "a scatola grigia". La prima applicazione a SCMT (Sistema Controllo Marcia Treni) è descritta in [12], mentre una successiva estensione con lo scopo di istanziare automaticamente prove astratte su impianti reali per i sistemi ACS (Apparato Centrale Statico) è descritta in [13]. Modelli comportamentali basati su macchine a stati finiti astratte, inoltre, assistono gli ingegneri della determinazione dei percorsi minimi che coprano tutte le combinazioni significative di variabili di stato e di ingresso (fig. 3b) [13]. Tale approccio è stato impiegato nelle verifiche funzionali di sistema per tutti i nuovi impianti ERTMS/ETCS, a partire dalla linea AV Roma-Napoli.

Quello che si ottiene è una procedura di *testing* ibrida, che abilita diversi automatismi e consente di verificare anche la coerenza dei requisiti, in cui i modelli (in tal caso prevalentemente semi-formali) giocano un ruolo di fondamentale importanza. In definitiva, la verifica basata su modelli consente di incrementare il numero di difetti rilevati a parità di tempo e risorse impiegate, renderne più veloce la correzione ed automatizzare la generazione dei casi di test.

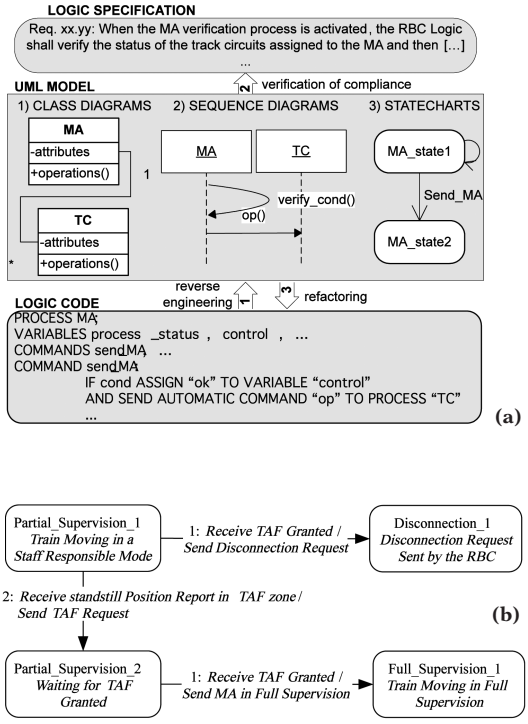

Fig. 3 - Modelli di supporto alle verifiche funzionali statiche (a) e dinamiche (b). *Support models for static (a) and dynamic (b) functional verifications.*

5. Analisi del rischio security

Gli attentati terroristici avvenuti negli ultimi anni, che hanno avuto in diversi casi come obiettivo infrastrutture ferroviarie o metropolitane, hanno portato alla ribalta le problematiche di protezione di tali sistemi nei confronti di minacce esterne di origine prevalentemente dolosa. Oltre al terrorismo, la categoria comprende eventi naturali e atti vandalici; questi ultimi, anche se generalmente non mietono vittime, comportano danni notevoli ai gestori delle infrastrutture.

E' fondamentale far precedere al progetto di sistemi di protezione un'attività di analisi che consenta di valutare in modo il più possibile preciso il rischio a cui il sistema è soggetto, in modo da predisporre gli interventi di mitigazione in funzione del bilancio costi/benefici. Il rischio è una combinazione di tre fattori legati a ciascuna minaccia: frequenza di accadimento, vulnerabilità (del sistema nei confronti della minaccia), danno (ovvero stima delle conseguenze). Ognuno di questi fattori, per altro interdipendenti, richiede opportuni modelli di valutazione affinché sia stimato in modo quantitativo. La stima analitica, d'altra parte, è indispensabile per affinare la precisione dei risultati ed effettuare eventuali ottimizzazioni automatiche sul dimensionamento dei meccanismi di protezione, come descritto nel riferimento [15]

evaluate the risk that the system is subject to, in order to predict the effectiveness of protection systems and other mitigation interventions in terms of cost/benefits. The risk is a combination of three factors which are related to each threat: frequency of occurrence, vulnerability (of the system against the threat), damage (i.e. evaluation of the consequences). Each of these possibly interdependent factors requires appropriate models in order to be evaluated in a quantitative way. The analytic estimation, on the other hand, is essential to improve the precision of the results and to perform possible automatic optimisations on the design of the protection mechanisms, as described in reference [15] considering the case study of a generic metro railway system.

Fig. 4 shows a possible approach to the modelling of risk which requires the construction of models expressed in different formalisms: the determination of the frequency *P* can be based on the correlation of statistical data through *Bayesian Networks*; the evaluation of the vulnerability *V* can be performed by means of *Generalised Stochastic Petri Nets*, which allow us to take into account both the temporal evolution of the threats and the laten-

considerando il caso di studio di un generico sistema di trasporto metropolitano.

La fig. 4 mostra un possibile approccio alla modellazione del rischio che richiede la costruzione di modelli espressi in diversi formalismi: la determinazione della frequenza *P* può basarsi sulla correlazione di dati statistici attraverso modelli bayesiani; la valutazione della vulnerabilità *V* può essere effettuata attraverso modelli a reti di Petri stocastiche, che consentono di tener conto sia dell'evoluzione temporale delle minacce che delle latenze di rilevamento e di intervento; la valutazione del danno *D* può basarsi su alberi degli eventi (*Event Trees*), che consentono di prevedere l'entità delle conseguenze modellando dipendenze causa-effetto.

Modelli che tengano conto in modo più dettagliato delle dinamiche di evoluzione delle minacce possono essere adottati nel contesto di studio delle infrastrutture critiche, e ciò consente anche di evidenziare le interdipendenze dei sistemi ferroviari con le altre infrastrutture interagenti (ad esempio, le reti di distribuzione elettrica o quelle di telecomunicazioni) [16].

Metodi per l'analisi attraverso approcci multi-formalismo degli attributi di security sono in corso di studio. Uno degli obiettivi è quello di utilizzare librerie di modelli modulari che opportunamente istanziati e composti tra loro consentano con poco sforzo di valutare ed ottimizzare in modo automatico gli attributi di security del sistema, tenendo conto di eventuali vincoli esterni.

6. Rilevamento di minacce in tempo reale

Un'ulteriore interessante applicazione dei modelli consiste nel rilevamento in tempo reale di minacce, in applicazioni che possono andare dalla diagnostica, alla prognostica, al rilevamento precoce di attacchi terroristici anche di tipo strategico, al monitoraggio di parametri ambientali per realizzare sistemi di allerta precoce e supporto alle decisioni. In tali applicazioni, i modelli realizzano il motore di rilevamento che fonde dati sensoriali eterogenei alla ricerca di *pattern* noti di minacce, preventivamente memorizzati in una specifica base dati secondo un opportuno linguaggio di specifica di eventi composti.

Un requisito importante, in tal caso, è la possibilità di reazione in tempo reale, che richiede modelli compatti e/o formalismi caratterizzati da efficienza risolutiva elevata. A tal scopo, possono essere impiegati formalismi determi-

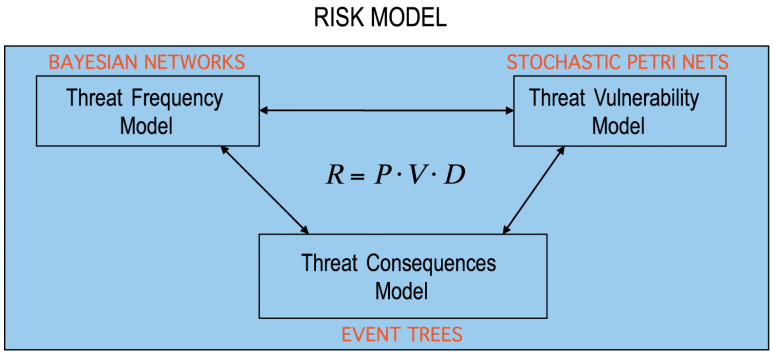

Fig. 4 - Valutazione del rischio basata su diversi formalismi. *Risk evaluation using different formalisms.*

cy of detection and intervention; the evaluation of damage *D* can be based on *Event Trees*, which allow the evaluation of the consequences based on cause/effect dependencies.

Models taking into account the evolution dynamics of the threats in a more detailed manner can be adopted in order to highlight the interdependences of the railway system with the other interacting infrastructures (for example, the networks of electrical distribution and telecommunications) [16].

Multi-formalism modelling approaches for the analysis of security attributes are being studied. One of the objectives is to use libraries of modular models which can be conveniently composed to allow the evaluation and automatic optimisation of security attributes taking into account possible external constraints.

6. Real-time threat detection

A further interesting application of models is the real-time detection of threats in applications including diagnostics, prognostics, early identification of terrorist attacks and environmental monitoring, in order to build early warning and decision support systems. In those applications, the models are necessary to build the detection engine fusing heterogeneous sensor data to identify known threat *patterns*, previously stored in repositories using appropriate composite-event specification languages.

An important requirement, in this case, is the possibility of real-time operation, which needs compact models and/or formalisms featuring high solving efficiency. To that aim, deterministic or stochastic formalisms can be employed. For example, Event Trees belong to the first category, whose solvers are highly efficient. Unfortunately, deterministic formalisms in detection models allow the

nistici o probabilistici. Alla prima categoria appartengono, ad esempio, gli alberi degli eventi, i cui risolutori sono caratterizzati da un'efficienza elevata. Purtroppo l'impiego di formalismi deterministici nei modelli di rilevamento consente di stimare al più il livello di evoluzione di una minaccia, ma non permette di rilevare scenari che si discostano da quelli noti, né di fornire degli indici di confidenza sul rilevamento. Viceversa, l'impiego di euristiche basate su modelli bayesiani, già utilizzate peraltro nel contesto degli *Intrusion Detection Systems* per le reti di calcolatori, consente, tra le altre cose, di tener conto dell'affidabilità del dato, e quindi stimare il livello di attendibilità dell'evento rilevato. Di conseguenza, è possibile associare al risultato un indice probabilistico, in funzione della propagazione del livello di incertezza sia sui parametri che sulla struttura del modello.

Una rappresentazione semplificata di un sistema del tipo sopra descritto è riportata in fig. 5, mentre per una descrizione di maggior dettaglio si rimanda al riferimento [17]. Tale sistema è attualmente in fase prototipale e se ne prevede una integrazione all'interno dei sistemi di gestione della security al fine di correlare eventi elementari per gli scopi suddetti, il che consente anche di incrementare l'affidabilità del rilevamento basandosi su diversità e ridondanza dei sensori [18].

estimation of the level of evolution of threats, but do not allow the detection of scenarios which vary from those already known neither provide any information about the detection reliability. On the other hand, the employment of heuristics based on Bayesian models, already used in the context of computer networks *Intrusion Detection Systems*, allow us to take into account data uncertainty and therefore estimate the level of reliability of the detected event. As a consequence, it is possible to associate to the result a stochastic index which is function of model parametric and structural uncertainty.

A simplified representation of such a system is reported in fig. 5, while a description of higher detail can be found in reference [17]. The system is currently in the prototype phase but we foresee an integration inside the Ansaldo STS Security Management System (SMS) in order to correlate basic events to "sniff" suspect events and even to increase event detection reliability basing on sensor diverse redundancy [18].

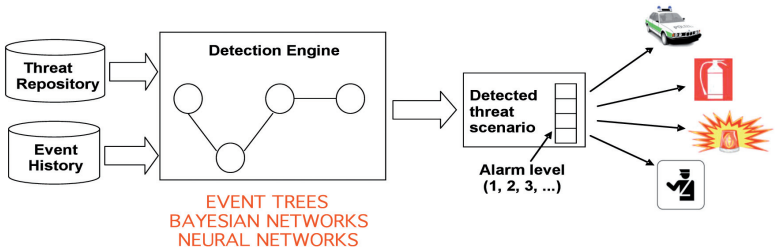

Fig. 5 - Modelli di rilevamento di minacce in tempo reale. *Real-time threat detection models.*

7. Conclusioni e sviluppi futuri

In questo articolo abbiamo mostrato in un rapido excursus diversi approcci modellistici per valutazioni di affidabilità e sicurezza dei sistemi ferroviari e metropolitani, evidenziando alcuni utili paradigmi, quale quello della modellazione multi-formalismo. Quest'ultimo è un aspetto della modellazione multi-paradigma, che comprende anche i concetti di astrazione e trasformazione dei modelli da un formalismo ad un altro. I formalismi adottati sono prevalentemente di tipo grafico, abbastanza diffusi perché tipicamente potenti e facili da usare. Non abbiamo affrontato in modo esplicito in questo lavoro la problematica della verifica di proprietà sui modelli (*model-checking* [19]) che è resa possibile da alcuni formalismi di modellazione basati sullo spazio di stato (si veda anche [20]).

Si è visto come, in generale, approcci basati su modelli siano impiegabili in molteplici applicazioni e consentano un elevato livello di rigore nella rappresentazione e precisione nella valutazione dei risultati. Inoltre, essi si prestano a tecniche di sviluppo modulari, eventualmente attraverso librerie di modelli predefiniti integrabili tramite opportuni operatori di composizione. Diverse sono le li-

7. Conclusions and future developments

In this article we have briefly addressed different modelling approaches for the evaluation of reliability, safety and security of rail-based transit systems, highlighting some useful paradigms, including multi-formalism modelling. The latter is an aspect of multi-paradigm modelling, which also includes the concepts of model abstraction and transformation. The formalisms adopted are predominantly graph-based and rather widespread, being powerful and easy to use. We have not tackled in this paper the problems of the verification of properties on the models (*model-checking* [19]), which is enabled by certain formalisms based on state-space analysis (see also [20]).

We have shown that, generally speaking, approaches based on models are employable in multiple applications and enable a higher precision in system representation and results evaluation. Furthermore, they allow for modular development techniques, possibly through libraries of sub-models which can be integrated by means of com-

nee di ricerca ancora aperte affinché l'impiego di tecniche avanzate divenga una pratica comune in contesti industriali. Tra queste, oltre agli aspetti teorici legati alla composizione di modelli eterogenei, ci sono quelli tecnologici legati alla risoluzione distribuita tramite tecniche di *work-flow management* [21].

Infine, esistono tutta una serie di nuove applicazioni, tra cui quelle di *security* [22], che rappresentano un banco di prova stimolante per approcci di modellazione avanzati, i quali risultano indispensabili dal momento che la complessità dei problemi è tale da rendere le tecniche tradizionali inadeguate o poco efficaci.

position operators. There are several still-open research areas related to those topics, which aim at making the employment of advanced techniques a common practice in industry. Included in those areas there are the theoretical aspects of heterogeneous model composition and the technological aspects related to the distributed simulation through *work-flow management* techniques [21].

Finally, there exist many recent applications, including infrastructure *security* [22], which represent challenging tests for advanced modelling approaches, being essential when the complexity of the problems is such to make traditional techniques inadequate or poorly effective.

BIBLIOGRAFIA – *REFERENCE*

[1] CENELEC: EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999.

[2] D.M. Nicol, W.H. Sanders, K.S. Trivedi, *"Model-based evaluation: from dependability to security",* in Dependable and Secure Computing, IEEE Transactions on, Vol.1, Issue 1, 2004: pp. 48- 65.

[3] F. Flammini, N. Mazzocca, V. Vittorini, *"Modelli per l'analisi di sistemi critici",* in Mondo Digitale, n. 3, Settembre 2009: pp. 11-21.

[4] UNISIG: ERTMS/ETCS Class 1 Issue 2.2.2 Subset 026, 2002.

[5] W.H. Sanders, *"Integrated Frameworks for Multi-Level and Multi-Formalism Modeling",* in Proc. 8th Intl. Workshop on Petri Nets and Performance Models, 1999: p. 2.

[6] F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini, *"Modelling 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, ESREL'06, Estoril, Portugal, September 18-22, 2006: pp. 2675-2683.

[7] F. Flammini, M. Iacono, S. Marrone, N. Mazzocca, *"Using Repairable Fault Trees for the evaluation of design choices for critical repairable systems",* in Proceedings of the 9th IEEE Symposium on High Assurance Systems Engineering, HASE'05, Heidelberg, Germany, October 12-14, 2005: pp. 163-172.

[8] A. Zimmermann, G. Hommel, *"Towards modeling and evaluation of ETCS real-time communication and operation",* in Journal of Systems and Software, Vol. 77, Issue 1, July 2005: pp. 47-54.

[9] A.M. Amendola, L. Impagliazzo, P. Marmo, G. Mongardi, G. Sartore, *"Architecture and Safety Requirements of the ACC Railway Interlocking System",* IEEE Proc. 2nd Annual Int. Computer Performance & Dependability Symposium (IPDS'96), Urbana Champaign, IL, USA, 1996: pp. 21-29.

[10] F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini, *"A new modelling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance",* in Reliability Engineering & System Safety (RESS), Vol. 94, Issue 9, September 2009: pp. 1422–1432.

[11] C. Abbaneo, F. Flammini, A. Lazzaro, P. Marmo, N. Mazzocca, A. Sanseviero, *"UML Based Reverse Engineering for the Verification of Railway Control Logics",* in IEEE Proc. of Dependability of Computer Systems, DepCoS'06, Szklarska Por´ba, Poland, May 25-27, 2006: pp. 3-10.

[12] G. De Nicola, P. di Tommaso, R. Esposito, F. Flammini, P. Marmo, A. Orazzo, *"A Grey-Box Approach to the Functional Testing of Complex Automatic Train Protection Systems",* in LNCS Vol. 3463: The Fifth European Dependable Computing Conference, EDCC-5, Budapest, Hungary, April 20-22, 2005: pp. 305-317.

[13] F. Flammini, N. Mazzocca, A. Orazzo, *"Automatic instantiation of abstract tests to specific configurations for large critical control systems",* in Journal of Software Testing, Verification & Reliability (STVR), Vol. 19, Issue 2, 2009: pp. 91-110.

[14] F. Flammini, P. di Tommaso, A. Lazzaro, R. Pellecchia, A. Sanseviero, *"The Simulation of Anomalies in the Functional Testing of the ERTMS/ETCS Trackside System"*, in Proc. 9th IEEE Symposium on High Assurance Systems Engineering, HASE'05, Heidelberg, Germany, October 12-14, 2005: pp. 131-139.

[15] F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola, *"Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures"*, in Proc. 3rd International Workshop on Critical Information Infrastructures Security, CRITIS'08, LNCS 5508, 2009: pp. 180-189.

[16] F. Flammini, N. Mazzocca, C. Pragliola, V. Vittorini, *"A Study on Multiformalism Modelling of Critical Infrastructures"*, in Proc. 3rd International Workshop on Critical Information Infrastructures Security, CRITIS'08, LNCS 5508, 2009: pp. 336-343.

[17] F. Flammini, A. Gaglione, N. Mazzocca, V. Moscato, C. Pragliola, *"On-line integration and reasoning of multi-sensor data to enhance infrastructure surveillance"*, in Journal of Information Assurance and Security (JIAS), Vol. 4, Issue 2, 2009: pp. 183-191.

[18] G. Bocchetti, F. Flammini, A. Pappalardo, C. Pragliola, *"Dependable integrated surveillance systems for the physical security of metro railways"*, in Proc. 3rd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC 2009), 30 August - 2 September, 2009, Como, Italy.

[19] A. Cimatti, F. Giunchiglia, G. Mongardi, D. Romano, F. Torielli, P. Traverso, *"Formal Verification of a Railway Interlocking System using Model Checking"*, in Journal on Formal Aspects in Computing, Vol.10, 1998: pp. 361-380.

[20] F. Senesi, R. Malangone, A. Piccolo, V. Galdi, *"Utilizzo di linguaggi formali per l'analisi e la valutazione delle specifiche di test del sistema ERTMS della rete italiana ad alta velocità"*, in Ingegneria Ferroviaria, Dicembre 2006, p. 957.

[21] G. Di Lorenzo, F. Flammini, M. Iacono, S. Marrone, F. Moscato, V. Vittorini, *"The software architecture of the OsMoSys multisolution frame work"*, in Proc. 2nd International Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS'07, Nantes, France, October 23-25, 2007: pp. 1-10.

[22] F. Flammini, N. Mazzocca, C. Pragliola, *"Protezione delle infrastrutture di trasporto su ferro"*, in Safety & Security, N. 8, Marzo 2008: pp. 12-16.