IEEE Control Systems Society
Technical Committee on Discrete Event Systems

Newsletter October 2022

Editor: Kai Cai
Chair, IEEE CSS Technical Committee on DES
Professor
Department of Core Informatics, Osaka Metropolitan University
3-3-138 Sugimoto, Sumiyoshi-ku, Osaka 558-8585, Japan

Phone: (+81) 6-6605-2703
Email: cai@omu.ac.jp
Website: https://www.control.eng.osaka-cu.ac.jp

Welcome to the 2022 October issue of the newsletter, also available online at
http://ieeecss.org/tc/discrete-event-systems/newsletters

Editorial

You are welcome to submit new items to the newsletter (topics including schools, workshops, sessions, conferences, journals, books, software, positions). Also please encourage relevant colleagues and students to subscribe to this newsletter.

- To **submit a new item**, please use the following website:
  https://www.control.eng.osaka-cu.ac.jp/miscellaneous/css-tc-des/submission
  or email to cai@eomu.ac.jp.
- To **subscribe**, please email to cai@omu.ac.jp.
- To **unsubscribe**, please reply to this email with the subject line UNSUBSCRIBE.

Contents

1 Selections of Journal Publications

Contributed by: Xiang Yin (yinxiang@sjtu.edu.cn)

1.1. Discrete Event Dynamic Systems Theory and Applications

Volume: 32, Issue: 3, October 2022

- **Epistemic interpretations of decentralized discrete-event system problems**
  Authors: Richard Ean ; Karen Rudie
  Abstract: This paper presents epistemic characterizations to co-observability conditions in decentralized supervisory control of discrete-event systems. The logical characterizations provide more intuitive interpretations of the various co-observability conditions, and make immediately apparent the relations between the conditions. Closures under set union of some of the conditions are also discussed.

- **Diagnosability verification using LTL model checking**
  Authors: Thiago M. Tuxi ; Lilian K. Carvalho ; Eduardo V. L. Nunes ; Antonio E. C. da Cunha
  Abstract: One of the challenges of fault diagnosis is to verify diagnosability of systems with huge state space efficiently. Model checking approaches have the potential to analyze such systems efficiently. In this work, we propose a model checking approach to deal with the problem of the diagnosability verification. We define the diagnosability property in the transition system framework. To check this property, we describe it by using an unique linear temporal logic (LTL) formula. Our approach can be carried out in model checker tools for formal verification of models, such as SPIN and NuSMV. To illustrate the efficiency of our approach we perform some experiments. First, we consider a railway level crossing benchmark, comparing the results of our approach in SPIN and NuSMV with the results found using DESLab and Supremica tools. Then, we perform an exploratory statistical analysis comparing the average size of verifiers computed with our approach in SPIN with the average size of verifiers (it number of states plus transitions) computed with DESLab, which is a tool for diagnosability verification of Discrete Event Systems (DES) that uses the same foundation idea.

- **Detectability of labeled weighted automata over monoids**
  Authors: Kuize Zhang
  Abstract: In this paper, by developing appropriate methods, we for the first time obtain characterization of four fundamental notions of detectability for general labeled weighted automata over monoids (denoted by $\mathcal{A}^{\mathfrak{M}}$ for short), where the four notions are strong (periodic) detectability (SD and SPD) and weak (periodic) detectability (WD and WPD). The contributions of the current paper are as follows. Firstly, we formulate the notions of concurrent composition, observer, and detector for $\mathcal{A}^{\mathfrak{M}}$. Secondly, we use the concurrent composition to give a necessary and sufficient condition for SD, use the detector to give a necessary and sufficient condition for SPD, and use the observer to give necessary and sufficient conditions for WD and WPD, all for general $\mathcal{A}^{\mathfrak{M}}$ without any assumption. Thirdly, we prove that for a labeled weighted automaton over monoid $(\mathbb{Q}^k, +)$ (denoted by $\mathcal{A}^{\mathbb{Q}^k}$), its concurrent composition, observer, and detector can be computed in NP, 2-EXPTIME, and 2-EXPTIME, respectively, by developing novel connections between $\mathcal{A}^{\mathbb{Q}^k}$ and the NP-complete exact path length problem (proven by [Nykänen and Ukkonen, 2002]) and a subclass of Presburger arithmetic. As a result, we prove that for $\mathcal{A}^{\mathbb{Q}^k}$, SD can be verified in coNP, while SPD, WD, and WPD can be verified in 2-EXPTIME. Particularly, for $\mathcal{A}^{\mathbb{Q}^k}$ in which from every state, a distinct state can be reached through some unobservable, instantaneous path, detector $\mathcal{A}^{\mathbb{Q}^k}_{det}$ can be computed in NP, and SPD can be verified in coNP. Finally, we prove that the problems of verifying SD and SPD of deterministic, deadlock-free, and divergence-free $\mathcal{A}^{\mathbb{N}}$ over monoid $(\mathbb{N}, +)$ are both coNP-hard. The original methods developed in this paper will provide foundations for characterizing other fundamental properties (e.g., diagnosability and opacity) in labeled weighted automata over monoids. In addition, in order to differentiate labeled weighted automata over monoids from labeled timed automata, we also initially explore detectability in labeled timed automata, and prove that the SD verification problem is PSPACE-complete, while WD and WPD are undecidable.

- **Observation-assisted heuristic synthesis of covert attackers against unknown supervisors**
  Authors: Liyong Lin ; Ruochen Tai ; Yuting Zhu ; Rong Su
  Abstract: In this work, we address the problem of synthesis of covert attackers in the setup where the model of the plant is available, but the model of the supervisor is unknown, to the adversary. To compensate the lack of knowledge on the supervisor, we assume that the adversary has recorded a (prefix-closed) finite set of observations of the runs of the closed-loop system, which can be used for assisting the synthesis. We present a heuristic algorithm for the synthesis of covert damage-reachable attackers, based on the model of the plant and the (finite) set of observations, by a transformation into solving an instance of the partial-observation supervisor synthesis problem. The heuristic algorithm developed in this paper may allow the adversary to synthesize covert attackers without having to know the model of the supervisor, which could be hard to obtain in practice. For simplicity, we shall only consider covert attackers that are able to carry out sensor replacement attacks and actuator disablement attacks. The effectiveness of our approach is illustrated on a water tank example adapted from the literature.
- **Max-plus steady states in discrete event dynamic systems with inexact data**
  Authors: Helena Myková ; Ján Plavka
  Abstract: Max-plus algebra is defined as the set of all real numbers with two binary operations (maximum and addition). This combination of the operations forms a very applicable tool for the investigation of systems working in discrete steps (discrete event dynamic systems). The search for the steady states in such systems leads to the study of the eigenvectors of the production matrix in the corresponding max-plus algebra. A vector x is said to be an eigenvector of a square matrix A if $A \otimes x = \lambda \otimes x$ for some $\lambda \in \mathbb{R}$. In real systems, the input values are usually taken to be in some interval. This paper investigates the properties of eigenspaces for vectors with interval (inexact) coefficients. We suppose that an interval vector X can be split into two subsets according to a forallexists quantification of its interval entries, i.e., $X = X^{\forall} \oplus X^{\exists}$. If for any vector of $X^{\forall}$ there is at least one vector of $X^{\exists}$ such that their vector maximum is an eigenvector of A, then X is said to be a λAE-eigenvector. Analogously, if there is at least one vector of $X^{\exists}$ such that for any vector of $X^{\forall}$ their vector maximum is an eigenvector of A, then X is said to be a λAE-eigenvector. The properties of such eigenvectors are studied and their characterizations by equivalent conditions are presented. Polynomial and pseudopolynomial algorithms for checking some types of $\lambda EA/\lambda AE$-eigenvectors are suggested.
- **Correction to: Probabilistic state estimation for labeled continuous time Markov models with applications to attack detection**
  Authors: Dimitri Lefebvre ; Carla Seatzu ; Christoforos N. Hadjicostis ; Alessandro Giua

Back to the contents

1.2. IEEE Transactions on Automatic Control

Volume: 67, Issue: 10, October 2022

- **Extended Insertion Functions for Opacity Enforcement in Discrete-Event Systems**
  Authors: Xiaoyan Li ; Christoforos N. Hadjicostis ; Zhiwu Li
  Abstract: Opacity is a confidentiality property that holds if certain secret behavior of a system, typically represented by a predicate, cannot be revealed under any system evolution. Among other proposed methodologies, when opacity is violated, it can be enforced using insertion mechanisms, i.e., by inserting symbols before an actual system output (in real time as the system evolves) in order to replace observation sequences that lead to opacity violations with observation sequences that can be generated by system behavior that does not violate opacity. This article focuses on opacity enforcement in discrete-event systems modeled with finite-state automata and proposes an extended insertion mechanism that can enforce opacity in a practical manner to a wide class of systems by inserting symbols before and after an actual system output. This article also introduces event insertion constraints that require only certain specific symbols to be inserted before and after an actual system output. For each case, we obtain a necessary and sufficient condition (based on

the construction of an appropriate verifier) for opacity enforceability using the proposed extended insertion mechanism and devise a pertinent extended insertion strategy.

- **Stochastic Failure Prognosis of Discrete Event Systems**
  Authors: Jun Chen ; Ratnesh Kumar
  Abstract: This article studies the prognosis of failure, i.e., its prediction prior to its occurrence, in stochastic discrete event systems. Prior work has focused on the definition and offline verification of m-steps stochastic-prognosability, or S_m-prognosability, which allows the prediction of a fault at least m-steps in advance. This article complements the existing work by proposing an algorithm for the computation of online failure prognoser. The proposed algorithm reduces the condition for issuing an affirmative prognostic decision to verification condition of a safety property of a Markov chain. We discuss how such a verification condition can be computed using a finitely terminating algorithm.

- **Prognosability Analysis and Enforcement of Bounded Labeled Petri Nets**
  Authors: Ning Ran ; Jinyuan Hao ; Carla Seatzu
  Abstract: In this article, we deal with two problems related to bounded labeled Petri nets (PNs), namely prognosability analysis and enforcement. The solution we propose is based on a single tool, called prognosability verifier. Such a tool uses the notion of basis marking that avoids the exhaustive enumeration of all the reachable markings. This leads to advantages in terms of computational complexity that may be enormous in certain real applications. Finally, the enforcement problem can be solved associating a cost with each sensor eventually added to the system. A systematic way to compute a solution that minimizes the total cost of the new sensors while guaranteeing prognosability of the resulting system, is computed using linear integer programming.

- **Combining Online Diagnosis and Prognosis for Safe Controllability**
  Authors: Ana T. Y. Watanabe ; André B. Leal ; José E. R. Cury ; Max H. de Queiroz
  Abstract: In this article, we combine fault diagnosis and prognosis to generalize the notion of safe controllability of discrete-event systems. To do so, we reformulate the notions of safe diagnosability, prognosability, safe controllability by diagnosis, and safe controllability by prognosis in the context of strings. Moreover, we combine these notions to introduce the concept of safe controllability by diagnosis or prognosis, or simply DP-safe controllability. We show that a language can be DP-safe controllable even if it is not safe controllable either only by diagnosis or only by prognosis. Thus, the DP-safe controllability can be considered a generalization of the safe controllability concept found in the literature. If a DES is DP-safe controllable, to achieve fault tolerance using an active approach, reconfiguration actions could be forced based not only on online fault diagnosis, but also on online fault prognosis. Thus, our approach outperforms the previous ones, since it provides additional control options to keep the system away from forbidden zones and to switch from the nominal supervisor to a postfault-detection supervisor designed to achieve postfault performance objectives. Necessary and sufficient conditions for DP-safe controllability are presented and an example is used to illustrate the introduced concepts.

- **Temporal Logic Trees for Model Checking and Control Synthesis of Uncertain Discrete-Time Systems**
  Authors: Yulong Gao ; Alessandro Abate ; Frank J. Jiang; Mirco Giacobbe ; Lihua Xie ; Karl Henrik Johansson
  Abstract: We propose algorithms for performing model checking and control synthesis for discrete-time uncertain systems under linear temporal logic (LTL) specifications. We construct temporal logic trees (TLTs) from LTL formulae via reachability analysis. In contrast to automaton-based methods, the construction of the TLT is abstraction-free for infinite systems; that is, we do not construct discrete abstractions of the infinite systems. Moreover, for a given transition system and an LTL formula, we prove that there exist both a universal TLT and an existential TLT via minimal and maximal reachability analysis, respectively. We show that the universal TLT is an underapproximation for the LTL formula and the existential TLT is an overapproximation. We provide sufficient conditions and necessary conditions to verify whether a transition system satisfies an LTL formula by using the TLT approximations. As a major contribution of this work, for a controlled transition system and an LTL formula, we prove that a controlled TLT can be constructed

from the LTL formula via a control-dependent reachability analysis. Based on the controlled TLT, we design an online control synthesis algorithm, under which a set of feasible control inputs can be generated at each time step. We also prove that this algorithm is recursively feasible. We illustrate the proposed methods for both finite and infinite systems and highlight the generality and online scalability with two simulated examples.

- **Probably Approximately Correct Learning in Adversarial Environments With Temporal Logic Specifications**
  Authors: Min Wen ; Ufuk Topcu
  Abstract: Reinforcement learning (RL) algorithms have been used to learn how to implement tasks in uncertain and partially unknown environments. In practice, environments are usually uncontrolled and may affect task performance in an adversarial way. In this article, we model the interaction between an RL agent and its potentially adversarial environment as a turn-based zero-sum stochastic game. The task requirements are represented both qualitatively as a subset of linear temporal logic (LTL) specifications, and quantitatively as a reward function. For each case in which the LTL specification is realizable and can be equivalently transformed into a deterministic Büchi automaton, we show that there always exists a memoryless almost-sure winning strategy that is ε-optimal for the discounted-sum objective for any arbitrary positive ε. We propose a probably approximately correct (PAC) learning algorithm that learns such a strategy efficiently in an online manner with a priori unknown reward functions and unknown transition distributions. To the best of our knowledge, this is the first result on PAC learning in stochastic games with independent quantitative and qualitative objectives.

- **Reactive and Risk-Aware Control for Signal Temporal Logic**
  Authors: Lars Lindemann ; George J. Pappas ; Dimos V. Dimarogonas
  Abstract: The deployment of autonomous systems in uncertain and dynamic environments has raised fundamental questions. Addressing these is pivotal to build fully autonomous systems and requires a systematic integration of planning and control. We first propose reactive risk signal interval temporal logic (ReRiSITL) as an extension of signal temporal logic (STL) to formulate complex spatiotemporal specifications. Unlike STL, ReRiSITL allows to consider uncontrollable propositions that may model humans as well as random environmental events such as sensor failures. Additionally, ReRiSITL allows to incorporate risk measures, such as (but not limited to) the conditional value-at-risk, to measure the risk of violating certain spatial specifications. Second, we propose an algorithm to check if an ReRiSITL specification is satisfiable. For this purpose, we abstract the ReRiSITL specification into a timed signal transducer and devise a game-based approach. Third, we propose a reactive planning and control framework for dynamical control systems under ReRiSITL specifications.

Back to the contents

1.3. Automatica

Volume: 144, October 2022

- **Synthesis for observability of logical control networks**
  Authors: Kuize Zhang
  Abstract: Finite-state systems have applications in systems biology, formal verification and synthesis of infinite-state (hybrid) systems, etc. As deterministic finite-state systems, logical control networks (LCNs) consist of a finite number of nodes which can be in a finite number of states and update their states. In this paper, we investigate the synthesis problem for observability of LCNs based on state feedback with exogenous input by using the semitensor product proposed by Daizhan Cheng and the notion of observability graph (previously called weighted pair graph) proposed by us. We prove that if an unobservable LCN can be made observable by state feedback with exogenous input, then it can also be made observable by state feedback (without exogenous input, equivalent to state feedback with constant input). Furthermore, we give an upper bound on the number of state-feedback controllers that are needed to be tested in order to verify whether an unobservable LCN can be made observable by state feedback, and based on the procedure of obtaining the upper bound, we design an observability synthesis algorithm, by additionally com-

bining the ideas of a greedy algorithm and dynamic programming. These results open the study of observability synthesis in LCNs.

- **Robust predictability of stochastic discrete-event systems and a polynomial-time verification**
  Authors: Hui Liao ; Fuchun Liu ; NaiqiWu
  Abstract: The purpose of fault prediction of discrete-event systems (DESs) is to predict the occurrence of fault in advance such that some protective actions can be taken before the occurrence of the fault. The robust predictability issue under the framework of stochastic DESs (SDESs) with model uncertainty is studied. First, the notions of (ϵ, m)-robust predictability and robust predictability of SDESs are formalized. In general, a set of stochastic systems being robustly predictable can predict the occurrences of faults in the sense of probability. Then the robust predictor and robust verifier for performing the robust prediction are constructed from the given possible stochastic systems. Particularly, the necessary and sufficient conditions for (ϵ, m)-robust predictability and robust predictability of SDESs are proposed, and an approach is presented to verify the robust predictability of SDESs with polynomial-time complexity both in the state space and in the number of all possible models.

- **Deterministic supervisory control with flexible upper-bounds on observation delay and control delay**
  Authors: Weilin Wang ; Yanwei Zang ; Shigemasa Takai ; Lachlan L.H.Andrew ; Chaohui Gong
  Abstract: This paper considers supervisory control of discrete event systems with observation delay and control delay. We first extend the formulation of networked supervisory control in the literature by allowing both the upper bound of observation delay and the upper bound of control delay to vary among different event strings, and accommodating dynamic observation in which the past influences whether or not an occurrence of an event is observable. We then combine observation delay and control delay and prove that satisfying both controllability and delay observability over the combined delay is necessary and sufficient for the existence of a supervisor by which the desired language can be obtained deterministically. After that, we reduce the type of problems concerning the networked supervisory control to the corresponding type of problems concerning traditional supervisory control without any delay on observation or control. As an immediate application, the verifier of observability can be used to test the corresponding delay observability. Finally, this reduction is used to leverage methods for minimizing sensor activations for supervisory control without control delay to minimize sensor activations with control delay.

- **Reinforcement learning with algorithms from probabilistic structure estimation**
  Authors: Jonathan P. Epperlein ; Roman Overko ; Sergiy Zhuk ; Christopher King ; Djallel Bouneffouf ; Andrew Cullen ; Robert Shorten
  Abstract: Reinforcement learning (RL) algorithms aim to learn optimal decisions in unknown environments through the experience of taking actions and observing the rewards gained. In some cases, the environment is not influenced by the actions of the RL agent, in which case the problem can be modeled as a contextual multi-armed bandit, and lightweight myopic algorithms can be employed. On the other hand, when the RL agents actions affect the environment, the problem must be modeled as a Markov decision process, and more complex RL algorithms are required, which take the future effects of actions into account. Moreover, in practice, it is often unknown from the outset whether or not the agents actions will impact the environment, and it is therefore not possible to determine which RL algorithm is most fitting. In this work, we propose to avoid this difficult decision entirely and incorporate a choice mechanism into our RL framework. Rather than assuming a specific problem structure, we use a probabilistic structure estimation procedure based on a likelihood-ratio (LR) test to make a more informed selection of the learning algorithm. We derive a sufficient condition under which myopic policies are optimal, present an LR test for this condition, and derive a bound on the regret of our framework. We provide examples of real-world scenarios where our framework is needed and provide extensive simulations to validate our approach.

Back to the contents

1.4. IEEE Transactions on Systems, Man, and Cybernetics: Systems

Volume: 52, Issue: 10, October 2022

- **Initial-State Observability of Mealy-Based Finite-State Machine With Nondeterministic Output Functions**

  Authors: Zhipeng Zhang ; Chengyi Xia ; Jun Fu ; Zengqiang Chen

  Abstract: In mobile systems or the failure detection applications, the output for some input event is state-dependent and nondeterministic after intermittent sensor failures or measurement uncertainties, which does not hold under the conventional observability hypothesis. In this article, such cases can be modeled by a Mealy-based finite-state machine (FSM) with nondeterministic output functions, and we investigate the initial-state observability by use of matrix semitensor product (matrix-STP). First, to characterize the nondeterministic output functions, a virtual state set consisting of stateevent pairs is introduced to obtain an augmented FSM. By resorting to the matrix-STP, the algebraic expression of augmented FSM is proposed. Subsequently, based on the newly constructed model, the initial-state observability can be verified by checking the distinguishability of state trajectories of the augmented FSM. Meanwhile, the necessary and sufficient condition for such initial-state observability is derived from a discriminant matrix consisting of polynomial elements. Finally, numerical examples show the validity of the proposed method. The current results are further conducive to explore the critical safety of cyberphysical systems in many real-world systems.

- **Verification of Nonblockingness in Bounded Petri Nets With Min-Max Basis Reachability Graphs**

  Authors: Chao Gu ; Ziyue Ma ; Zhiwu Li ; Alessandro Giua

  Abstract: This article proposes a semi-structural approach to verify the nonblockingness of a Petri net. We construct a structure, called minimal-maximal basis reachability graph (min-max-BRG): it provides an abstract description of the reachability set of a net while preserving all information needed to test if the net is blocking . We prove that a bounded deadlock-free Petri net is nonblocking if and only if its min-max-BRG is unobstructed , which can be verified by solving a set of integer constraints and then examining the min-max-BRG. For Petri nets that are not deadlock-free, one needs to determine the set of dead markings. This can be done with an approach based on the computation of maximal implicit firing sequences enabled by the markings in the min-max-BRG. The approach we developed does not require the construction of the reachability graph and has wide applicability.

Back to the contents

2 Conferences

Contributed by: Xiang Yin (yinxiang@sjtu.edu.cn)

2.1 **2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**
Prague, Czech Republic, October 9-12, 2022
https://ieeesmc2022.org/

2.2 **2022 IEEE Conference on Decision and Control (CDC)**
Cancun, Mexico, December 6-9, 2022
https://cdc2022.ieeecss.org/

2.3 **2023 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)**
San Antonio, USA, May 9-12, 2023
https://iccps.acm.org/2023/

2.4 **2023 American Control Conference (ACC)**
San Diego, USA, May 31 - June 2, 2023
https://acc2023.a2c2.org/

2.5 **2023 IFAC World Congress (IFAC)**
Yokohama, Japan, July 9-14, 2023
https://www.ifac2023.org/

Back to the contents

3 Books

3.1 Analysis and Control for Resilience of Discrete Event Systems

Authors: Joao Carlos Basilio, Christoforos N. Hadjicostis and Rong Su

Description: System resilience captures the ability of the system to withstand a major disruption within acceptable performance degradation and to recover within an acceptable time frame. In this monograph we consider two possible sources of major disruptions, i.e., component faults and cyber intrusions. A component fault is an indigenous activity that renders unavailability or inaccessibility of certain functions within a component, either permanently or temporarily. It typically generates safety and performance concerns. Cyber intrusion on the other hand is an exogenous activity that tampers privacy, confidentiality, availability, or integrity of the system. These two sources are not always independent from each other. For example, a cyber intrusion may trigger a component fault, whereas a component fault may open a door for cyber intrusion, e.g., by keeping it undetected. For cyber intrusion, we will focus on opacity, which describes the systems ability to hide certain secrets from an external observer (or eavesdropper), and sensor and actuator attacks that exploit the systems existing controller to generate undesirable behaviours.

In this monograph, we provide a detailed account of most recent research outcomes on fault diagnosis, opacity analysis and enhancement, and cyber security analysis and enforcement, within suitable discrete event system modelling frameworks. In each case, we describe basic problem statements and key concepts, and then point out the key challenges in each research area. After that, we present a thorough review of state-of-the-art techniques, and discuss their advantages and disadvantages. Finally, we highlight key research directions for further exploration.

ISBN: 978-1-68083-856-5
https://www.nowpublishers.com/article/Details/SYS-024

3.2 Introduction to Discrete Event Systems

Authors: Christos Cassandras and Stéphane Lafortune

Description: Christos Cassandras and Stéphane Lafortune are happy to announce the publication of the third edition of their textbook, Introduction to Discrete Event Systems, by Springer in November 2021. The first two editions of this popular textbook were published in 1999 (Kluwer Academic Publishers) and 2008 (Springer), respectively. This unique textbook comprehensively introduces the field of discrete event systems, offering a breadth of coverage that makes the material accessible to readers of varied backgrounds. The book emphasizes a unified modeling framework that transcends specific application areas, linking the following topics in a coherent manner: language and automata theory, supervisory control, Petri net theory, Markov chains and queueing theory, discrete-event simulation, and perturbation analysis and concurrent estimation techniques. The third edition is a superset of the second one, with new material added based on our teaching of discrete event systems courses at Boston University and at the University of Michigan, and they reflect active research trends in discrete event systems since the publication of the second edition.

Topics and features:
- detailed treatment of automata and language theory in the context of discrete event systems, including application to state estimation and diagnosis
- comprehensive coverage of centralized and decentralized supervisory control
- timed models, including timed automata and hybrid automata - stochastic models for discrete event systems and controlled Markov chains
- discrete event simulation - an introduction to stochastic hybrid systems
- sensitivity analysis and optimization of discrete event and hybrid systems
- new in the third edition: opacity properties, enhanced coverage of event diagnosis and of supervisory control under partial observation, overview of latest software tools, updated treatment of Infinitesimal Perturbation Analysis and of concurrent estimation

This proven textbook is essential to students and researchers in a variety of disciplines where the study of discrete event systems is relevant: control, communications, computer engineering, computer science, manufacturing engineering, transportation networks, operations research, and industrial engineering. This book is available through SpringerLink as an e-book (PDF and EPUB formats) or as a print-on-demand hard cover at https://link.springer.com/book/10.1007/978-3-030-72274-6 The e-book is available for free download at Springer subscribing institutions.

ISBN 978-3-030-72272-2 ISBN 978-3-030-72274-6 (eBook)
https://doi.org/10.1007/978-3-030-72274-6

3.3 Hybrid Dynamical Systems – Fundamentals and Methods

Authors: Hai Lin and Panos Antsaklis

Description: This book is based on courses on hybrid systems, cyber-physical systems, and formal methods taught by the authors in the past years. It is a graduate level textbook and provides an accessible and comprehensive introduction to the theory of hybrid systems with a balanced treatment on fundamentals and methods from both control theory and computer science. It also serves as a reference book for researchers in the fields of hybrid dynamical systems, cyber-physical systems, formal methods and robotics.

More information may be found at the books Springer webpage:

https://link.springer.com/book/10.1007/978-3-030-78731-8

Back to the contents

4 Software Tools

4.1 DESpot 1.10.0 Released

DESpot is a discrete-event system (DES) software, research tool. It supports both flat projects (collection of plant and supervisor DES), and Hierarchical Interface-Based Supervisory Control (HISC) projects.

DESpot 1.10.0 supports a number of new Features:

- DESpot now targets version 4.8.7 of the Qt libraries, RedHat Enterprise Linux 7.x, and MS Windows 10 with MS Visual Studios 2019.
- Support for defining template DES, and then instantiating multiple copies for flat or HISC projects.
- Now includes curved transition arrows for DES diagrams, and the ability to export DES diagrams to EPS.
- Support for verification of timed controllability, including BDD-based algorithms.
- Support for Fault-Tolerant (FT) Supervisory Control, including both timed and untimed controllability and nonblocking BDD-based algorithms, for several fault scenarios.
- Support for specifying decentralized supervisory control structure for a project, and verifying co-observability.

To find out more information and to download a copy, see: http://www.cas.mcmaster.ca/~leduc/DESpot.html

DESpot is open source software, released under the GNU General Public license (GPL), version 2.

DESpot is written in C++ and uses the QT GUI libraries. At the moment, DESpot is available as source code and as a Windows' installer. It runs under Linux, and Windows.

4.2 Eclipse ESCET™ version 0.7 release

The Eclipse Supervisory Control Engineering Toolkit (Eclipse ESCET) project provides a model-based approach and toolkit for the development of supervisory controllers. It includes the languages CIF, Chi and ToolDef. ESCET, initially developed by Eindhoven University of Technology, is since January 2020 an Eclipse Foundation open-source project. More information can be found on the toolkits website at https://www.eclipse.org/escet/.

In September 2022, ESCET version 0.7 has been released and can be downloaded from https://www.eclipse.org/escet/download.html. The main changes in this version are

- The CIF controller property checker can now also check whether controllers satisfy the confluence property.
- The CIF examples contain a new bridge example to showcase the real-world usage of CIF for synthesis-based engineering. Furthermore, two new CIF benchmarking models have been added.
- The CIF event-based language equivalence check tool now produces correct counter examples.
- The CIF to Supremica transformation precondition check has improved output and no longer crashes on reporting certain precondition violations. The preconditions themselves have not changed.
- The CIF text editor now has theming support, and comes with a dark theme in addition to the existing light theme. The text editor now automatically uses its dark theme when the Eclipse built-in dark theme is used, and uses a light theme otherwise.

The full ESCET release notes, including links to the language specific release notes and release notes from previous versions, are available from https://www.eclipse.org/escet/release-notes.html.

4.3 IDES: An Open-Source Software Tool

IDES, the discrete-event systems software tool in Karen Rudie's lab is now available as open-source software at https://github.com/krudie/IDES. More information on IDES can also be found at https://www.ece.queensu.ca/people/K-Rudie/qdes.html#fndtn-software.

4.4 MDESops

MDESops is an open-source tool written in Python for analysis and control of discrete event systems modeled as finite-state automata. It includes a growing set of operations on automata, including: (i) manipulation of models (e.g., parallel composition, observer); (ii) diagnosis and opacity verification; (iii) common supervisory control functions (e.g., computation of supremal controllable and normal sublanguages); and (iv) more advanced functions on synthesis of attackers and of resilient supervisors in the presence of sensor deception attacks. The repository is a Git server maintained by the EECS Department at the University of Michigan, USA. Download from https://gitlab.eecs.umich.edu/M-DES-tools/desops.

4.5 Supremica 2.7, New Version

The development team has just released a new version of Supremica, Waters/Supremica IDE 2.7.

Supremica is a DES and SCT drawing and calculation tool, that includes a multitude of efficient algorithms for modeling, verification, and synthesis of maximally permissive supervisors. In addition there are general algorithms for standard operations like synchronization, minimization, determinization, etc. Supremica also handles finite automata extended with bounded discrete variables. A feature-full simulation tool is also included.

New in this version:

- Conditional blocks or IF statements can now be created in the components list or on label blocks to allow conditional compilation of automata or events. They can also be used as an alternative to guard/action blocks.
- Update to Log4j 2.17.1 to avoid the Log4shell vulnerability.

Supremica is free to use for education and research; for commercial use, please contact fabian@chalmers.se. Download from www.supremica.org.

4.6 UltraDES 2.2 Release

UltraDES is an open-source library to the modeling, analysis and control of DES, written using C# in .NET Standard 2.0, which allows its use in multiple platforms, such as Windows, Linux, Mac, IOS, Android, so on. The library is under development at LACSED (Laboratory of Analysis and Control of Discrete Event Systems, at the Universidade Federal de Minas Gerais, Brazil) and has basic operations with automata as long as the monolithic, modular and local modular supervisory control (Alves et. al., 2017).

The main improvements of the UltraDES 2.2 version are:

- Supervisor Reduction Algorithm (Su and Wonham, 2004)
- Supervisor Localization (Cai and Wonham, 2010)
- Basic Petri Nets Functions (incidence matrix, coverability/reachability graph, Petri Net marking simulation, etc.)

Knowing that many researchers/students are not familiar with the C# language, we created an experimental python wrapper, that is less object oriented and easier to use.

Another initiative to improve the usability of UltraDES was the creation of a Web Application, developed using Blazor/WebAssembly, that allows the use of UltraDES online. This version is more limited in processing power and memory but it is useful for small examples and teaching.

We invite the community to download and contribute. Algorithms implemented may be integrated to the main distribution. Just let us know. Contact Lucas Alves lucasvra@ufmg.br or Patricia Pena ppena@ufmg.br for more information. Bugs should be informed using the UltraDES GitHub page.
Link: https://github.com/lacsed/UltraDES.

Back to the contents