IEEE Control Systems Society
Technical Committee on Discrete Event Systems

Newsletter July 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 July 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. IEEE Transactions on Automatic Control

Volume: 67, Issue: 7, July 2022

- **A Compact and Uniform Approach for Synthesizing State-Based Property-Enforcing Supervisors for Discrete-Event Systems**
  Authors: Rômulo Meira-Góes ; Jack Weitze ; Stéphane Lafortune
  Abstract: In this article, we are interested in the problem of synthesizing a partial observation supervisor for a discrete-event system such that it enforces a desired property. We introduce a compact and uniform approach to the problem of synthesizing state-based property-enforcing supervisors. A state-based property is a property that only depends on the current estimate of the past behavior of the system and does not depend on its future behavior. Previous work has introduced a uniform methodology to solve this problem through the construction of a finite structure called the all enforcement structure (AES), which captures a game between the supervisor and the environment. Although the AES is a powerful structure that includes all possible property-enforcing supervisors, its construction is computationally challenging since the number of states grows exponentially in the number of states and the number of events of the system. Our contribution is the definition of a compact AES that is equivalent to but computationally more efficient than the original AES. Specifically, the compact AES enjoys the same properties as the original AES with respect to synthesizing maximally permissive supervisors under the assumption of incomparable sets of controllable and observable events. We also provide experimental results to show the benefits of the compact AES over the original AES.
- **Design of Optimal Control Sequences in Petri Nets Using Basis Marking Analysis**
  Authors: Ziyue Ma ; Minqiang Zou ; Jiafeng Zhang ; Zhiwu Li
  Abstract: In this article, we develop an algorithm for designing an optimal control sequence in Petri nets, which drives a plant net from a source marking to a set of target markings without passing any pregiven forbidden markings. Such control sequences are useful in flexible reconfigurable automated systems, where a plant necessarily responds promptly to a request of reconfiguration. We develop a Dijkstra searching algorithm that is carried out in the basis marking space of a plant net instead of the conventional reachability space. Hence, only a small subset of the reachability set is explored, while the unpromising branches are reduced. Moreover, we propose a transition selecting rule to expose all forbidden trajectories and all first-met target markings during the searching process. The main advantage of the proposed method is wide applicability and low computational effort.
- **A Clustering Approach to Approximate the Timed Reachability Graph for a Class of Time Petri Nets**
  Authors: Jiazhong Zhou ; Dimitri Lefebvre ; Zhiwu Li
  Abstract: Timed extended reachability graphs (TERG) of time Petri nets abstract the temporal specifications and represent the feasible trajectories under the earliest firing policy. One drawback of such graphs is the rapid increase in the number of states with respect to time specifications. For this reason, approximations of TERG that remove some states have been studied in recent works. In this article, we improve the approximation of a TERG. New objectscalled verticesare defined to manipulate the time constraints and algorithms are proposed to cluster nearby vertices. A metric based on the time constraints is defined for this purpose and a cluster TERG of reduced size is obtained.
- **Stability of Discrete-Time Systems Under Restricted Switching via Logic Dynamical Generator and STP-Based Mergence of Hybrid States**
  Authors: Yuqian Guo ; Yuhu Wu ; Weihua Gui
  Abstract: In this article, we propose a novel technique for the stability analysis of discrete-time switched systems under constrained switching based on the semitensor product (STP) of matrices and vector-representation of logic. We assume that the admissible switching signals are generated by a logic dynamical system, referred to as the logic dynamical generator (LDG) of the admissible

switching. We demonstrate that switching with minimum dwell-time and restricted successors represent two special cases of this type, by constructing their respective LDGs. First, we transfer the LDG into algebraic form, based on the vector-representation of logic. Next, we merge the logic state of the LDG and the continuous state of the original switched system using the STP and derive the dynamics of the merged state; a switched system without constraints on switching. The stability of the switched system under constrained switching is equivalent to the stability of the merged system under arbitrary switching. Based on this, sufficient conditions for the asymptotical stability of nonlinear switched systems with analytic subsystems under constrained switching are obtained. Specifically, in the case of all subsystems being linear, necessary and sufficient conditions for asymptotical stability under constrained switching are proposed.

Back to the contents

1.2. Annual Reviews in Control

Volume: 53, 2022

- **Secure-by-construction synthesis of cyber-physical systems**
  Authors: Siyuan Liu ; Ashutosh Trivedi ; Xiang Yin ; Majid Zamani
  Abstract: Correct-by-construction synthesis is a cornerstone of the confluence of formal methods and control theory towards designing safety-critical systems. Instead of following the time-tested, albeit laborious (re)design-verify-validate loop, correct-by-construction methodology advocates the use of continual refinements of formal requirements connected by chains of formal proofs to build a system that assures the correctness by design. A remarkable progress has been made in scaling the scope of applicability of correct-by-construction synthesis with a focus on cyber-physical systems that tie discrete-event control with continuous environment to enlarge control systems by combining symbolic approaches with principled state-space reduction techniques. Unfortunately, in the security-critical control systems, the security properties are verified ex post facto the design process in a way that undermines the correct-by-construction paradigm. We posit that, to truly realize the dream of correct-by-construction synthesis for security-critical systems, security considerations must take center-stage with the safety considerations. Moreover, catalyzed by the recent progress on the opacity sub-classes of security properties and the notion of hyperproperties capable of combining security with safety properties, we believe that the time is ripe for the research community to holistically target the challenge of secure-by-construction synthesis. This paper details our vision by highlighting the recent progress and open challenges that may serve as bricks for providing a solid foundation for secure-by-construction synthesis of cyber-physical systems.

Back to the contents

1.3. IEEE Control Systems Letter

Volume: 6, Issue: 6, July 2022

- **Guest Editorial to the Special Section of L-CSS on Fragility and Resiliency in Cyber-Physical Discrete-Event Systems**
  Authors: Hadjicostis Christoforos N. ; Lafortune Stéphane ; Seatzu Carla
  Abstract: Fragility and resiliency have emerged as important research topics in the control of Cyber-Physical Systems (CPS), especially when the associated sensors and actuators may be compromised by malicious attackers. These problems have received increasing attention in the area of discrete event systems, where discrete abstractions of CPS are used to study resilient state estimation and supervisory control. A Call for Papers for this Special Section was issued in the fall of 2021, with a submission deadline of January 20, 2022. The submissions received were reviewed and revised according to the policies and timelines of L-CSS. Five Guest Associate Editors were invited to handle the submissions.
- **Privacy-Preserving POMDP Planning via Belief Manipulation**
  Authors: Wei Zheng; Taeho Jung; Hai Lin
  Abstract: The privacy issue has become one of the most critical concerns in cyber-physical systems (CPSs) as CPSs are vulnerable to information leakage. In particular, a passive intruder could infer the secret information of the system through observations, and the system may be critically

compromised or damaged once the intruder has high confidence on certain secret states. In this letter, we investigate the planning problem of a stochastic system in the presence of a passive eavesdropping intruder. In this system, the planner is modeled as a Markov decision process (MDP) who can access the state information and control the system transition. The intruder, who has a partial observation of the system state, is modeled as a hidden Markov model. The goal of the intruder is to infer the secrets of the system in terms of whether the current system is in some sensitive states, and the goal of the defender is to maximize the reward while preventing the intruder from inferring the secret. Distinct from existing work that embedded privacy as a part of the reward or utility function, we quantify privacy as a constraint for the planning. The problem is formulated as a constrained partially observable MDP (POMDP) planning problem and a belief state partition approach is proposed to solve the privacy-preserving planning problem via value iteration. Our observation is that the defender could prevent the intruder from inferring sensitive information via belief manipulation. However, the introduction of the privacy concern may sacrifice the system performance or even cause the problem to be infeasible. A necessary and sufficient condition is given to check the feasibility of the planning problem and examples are shown to illustrate our proposed algorithm.

Back to the contents

1.4. IEEE Transactions on Automation Science and Engineering

Volume: 19, Issue: 2, April 2022

- **Robust Fault Prognosis of Discrete-Event Systems Against Loss of Observations**
  Authors: Cuntao Xiao ; Fuchun Liu
  Abstract: This article investigates the robust fault prognosis of discrete-event systems (DESs) against the loss of observations of events. To solve this problem, a dilated automaton is generated from the plant by adding an unobservable transition attached to every event subject to loss of observations. We prove the equivalence between the robust prognosability of the plant model and the prognosability of the dilated model. In order to deal with unobservable cycles in the dilated model, a new necessary and sufficient condition of robust prognosability based on diagnoser is presented. Moreover, a polynomial algorithm for the verification of robust prognosability is proposed by constructing the verifier to search the existence of some cycle generated by a faulty trace and an unprognosable trace that run synchronously and keep the identical observation before the fault occurs. Our results generalize previous works on fault prognosis of DESs by taking the loss of observations into account. **Note to Practitioners:** The research in this article is motivated by the problem of fault prognosis in the manufacturing system. If some information used for prediction is lost, can engineers still make correct decisions about the occurrences of fault? This article aims to investigate the approach of assuring the accuracy and reliability of prediction by introducing the notion of robust prognosis. A polynomial-time algorithm of verifying the robust prognosability is proposed by constructing the tester automaton.
- **Diagnosability of Event Patterns in Safe Labeled Time Petri Nets: A Model-Checking Approach**
  Authors: Yannick Pencolé ; Audine Subias
  Abstract: Checking the diagnosability of a timed discrete-event system usually consists in determining whether a single fault event can always be identified with certainty after a finite amount of time. The aim of this article is to extend this type of analysis to more complex behaviors, called event patterns, and to propose an effective method to check diagnosability with the use of model-checking techniques. To do so, we propose to convert the pattern diagnosability problem into checking a linear-time property over a specific time Petri net. **Note to Practitioners:** This article is motivated by the problem of improving the monitoring and the supervision of systems, such as automated and robotized manufacturing systems. Based on a model of the system, this article proposes a method to assert with certainty whether the available set of sensors will always provide enough information to ensure that a complex and unexpected behavior has not happened in the system. The proposed method uses a publicly available model-checking tool to perform this analysis.

- **Crucial States Estimation in Radio Block Center Handover Using Petri Nets With Unobservable Transitions**
  Authors: Hao Lan ; Yin Tong ; Carla Seatzu
  Abstract: The radio block center (RBC) is one of the most essential ground systems in a high-speed train control system both in Europe and in China. The RBC handover procedure is an important function of RBC, which affects the transport efficiency, reliability and safety of railways. Analysis of crucial states in the RBC handover procedure is helpful to determine whether there are potential risks in the procedure, and to locate the fault in time when a fault occurs. In this paper, we study a property, called C-detectability, of the RBC handover. This property has been defined in discrete event systems and requires that the crucial states can be determined uniquely by observing the system output. Taking the RBC handover procedure in the Chinese train control system level 3 (CTCS-3) as an example, we first model the RBC handover procedure using Petri nets, which are a graphical and mathematical modeling tool to formalize the behavior of discrete event systems. Then, based on the notion of basis reachability graph, an efficient approach is used to check C-detectability of the Petri net modeling the handover procedure. **Note to Practitioners:** The railway system is a safety-critical system. System safety is essential to the railway system. It is necessary to provide formal methods to model the system and analyze its properties. The motivation of this work is to present a general modeling framework of railway systems for the crucial states estimation. The crucial states estimation of the railway system has not been discussed yet in the literature despite its importance due to its relationship with the safety of the railway. In particular, estimating the crucial states in the railway system helps to determine whether there are potential risks in the system. In this paper, we investigate a new state estimation property (C-detectability), which is related to fault diagnosis, marking estimation and fault identification. Future research will consider the use of timed Petri nets to increase the modeling power and to allow the performance analysis of the railway system.

Back to the contents

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

Volume: 52, Issue: 6, July 2022

- **On Optimal Supervisor Design for Discrete-Event Systems Modeled With Petri Nets via Constraint Simplification**
  Authors: YuFeng Chen ; YuTing Li ; ZhiWu Li ; NaiQi Wu
  Abstract: With integer linear programming problems (ILPPs) being formulated and solved, the existing approaches design optimal Petri-net supervisors via nonpure net structures, including self-loops and data inhibitor arcs. Nonpure net structures are powerful for control of Petri-net-modeled discrete-event systems. However, in the existing work, the formulated ILPPs contain a large number of constraints, which is computationally inefficient. In this article, we propose approaches that formulate ILPPs with fewer constraints such that the computational efficiency is significantly improved. To do so, in formulating ILPPs for optimal Petri-net controllers by using self-loops and data inhibitor arcs, we remove the reachability conditions for legal markings. By doing so, an obtained solution may result in some legal markings unreachable. To solve this problem, a novel technique is developed to design an optimal controller by modifying the initial marking and structure of the obtained supervisor. It is shown that, by the reduced ILPPs, one can find the same feasible solutions as that obtained by the existing work. Finally, the proposed approaches are demonstrated by examples.
- **Synchronization of an Array of Coupled Probabilistic Boolean Networks**
  Authors: Chi Huang ; Daniel W. C. Ho ; Jianquan Lu ; Wenjun Xiong ; Jinde Cao
  Abstract: Two synchronization problems, synchronization with probability one and synchronization in probability, are investigated for an array of coupled probabilistic Boolean networks (CPBNs). Compared with the former one, the in-probability problem considers a more general situation, in which synchronization can be achieved with a positive probability, instead of strictly 100%. It reflects the intrinsic randomness of biological systems. For both problems, some necessary and sufficient conditions are proposed, based on which two feasible algorithms are presented for checking

two kinds of synchronization, respectively. CPBNs can be seemed as a combination of coupled Boolean networks (CBNs) with assigned probabilities. There are also detailed discussions on the impact of the synchronism of CBNs on the two addressed synchronization problems. The existence of invariant synchronization subsets is studied, which deepens our understanding on the difference and difficulty of these problems. Finally, numerical simulations show the effectiveness of the theoretical results.

Back to the contents

2 Conferences

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

2.1 **2022 IEEE Conference on Control Technology and Applications (CCTA)**
Stazione Marittima, Trieste, Italy, August 23-25, 2022
https://acc2022.a2c2.org/

2.2 **2022 IEEE International Conference on Automation Science and Engineering (CASE)**
Mexico City, Mexico, August 20-24, 2022
http://www.case2022.org/

2.3 **2022 International Workshop on Discrete Event Systems (WODES)**
Prague, Czechia, September 7-9, 2022
https://wodes2022.math.cas.cz

2.4 **2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**
Prague, Czech Republic, October 9-12, 2022
https://ieeesmc2022.org/

2.5 **2022 IEEE Conference on Decision and Control (CDC)**
Cancun, Mexico, December 6-9, 2022
https://cdc2022.ieeecss.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 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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 coobservability.

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.

Back to the contents