IEEE Control Systems Society
Technical Committee on Discrete Event Systems

Newsletter **December 2023**

Editor: Xiang Yin
Chair, IEEE CSS Technical Committee on DES
Associate Professor
Department of Automation, Shanghai Jiao Tong University
SEIEE Building 2-443, Dongchuan Rd 800, Shanghai, 200240, China

Phone: (+86) 021-34204022
Email: yinxiang@sjtu.edu.cn
Website: http://xiangyin.sjtu.edu.cn

Welcome to the 2023 December issue of the newsletter, also available online at
https://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 email to yinxiang@sjtu.edu.cn.
- To **subscribe**, please email to yinxiang@sjtu.edu.cn.
- 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: 33, Issue: 4, December 2023

- **A multi-objective approach for manufacturing systems with multiple production routes based on supervisory control theory and heuristic algorithms**
  Authors: Lucas V. R. Alves ; Gustavo C. Rafael ; Lucas S. Batista ; Patrícia N. Pena
  Abstract: Heterogeneity among equipment in industrial production lines may have a major impact on energy consumption and makespan. The Supervisory Control Theory of discrete event systems proved to be especially useful to model the production system respecting its constraints and ensuring the safe execution on a real plant, such that an optimized production plan can be picked among the safe sequences. In this work, the makespan and the energy consumption minimization problem in discrete event systems with multiple production routes is addressed as a multi-objective problem. A multi-objective modeling is proposed, which considers the information regarding the power demanded by the system in each state of each equipment and the expected duration of each operation in the system. A dedicated Multi-Objective Variable Neighborhood Search (MOVNS) algorithm is also proposed to estimate an adequate set of trade-off solutions. A multi-criteria decision aid method is used to support the selection of an appropriate solution for the problem. The combination of the proposed modeling with both the MOVNS and a decision-making support has shown to be efficient regarding the solution of four test instances considered in this work.
- **On tolerance of discrete systems with respect to transition perturbations**
  Authors: Rômulo Meira-Góes ; Eunsuk Kang ; Stéphane Lafortune ; Stavros Tripakis
  Abstract: Control systems should enforce a desired property for both expected/modeled situations as well as unexpected/unmodeled environmental situations. Existing methods focus on designing controllers to enforce the desired property only when the environment behaves as expected. However, these methods lack discussion on how the system behaves when the environment is perturbed. In this paper, we propose an approach for analyzing discrete-state control systems with respect to their tolerance against environmental perturbations. We formally define this notion of tolerance and describe a general technique to compute it, for any given regular property. We also present a more efficient method to compute tolerance with respect to invariance properties. Moreover, we show that there exists an inherent trade-off between permissiveness and tolerance that we capture via Pareto optimality conditions. We also study the problem of synthesizing Pareto optimal controllers that achieve a minimum level of tolerance and permissiveness. We demonstrate our framework on examples involving surveillance protocols and robotic motion planning.
- **Multi-level control for multiple mobile robot systems**
  Authors: Elzbieta Roszkowska ; Piotr Makowski-Czerski ; Lukasz Janiec
  Abstract: This paper contributes with a multi-level, hierarchical control system for a fleet of mobile robots sharing a common 2D motion space. The system consists of three levels, with the top level being a supervisor based on a discrete representation of the Multiple Mobile Robot System (MMRS), in which robot motion processes are seen as sequences of stages. The supervisor controls centrally the changes of their stages by robots, ensuring their collision-, and deadlock-free concurrent movement. The intermediate control level supervises locally the execution of robot motion on individual stages in a manner consistent with the decisions of the top level. The lowest level, robot control, is responsible for motion execution as determined by the local supervisor. We capitalize on some earlier results concerning the supervisory control of MMRS and propose a common framework for three supervisory control models. Then we propose relevant solutions for the local supervisors, in particular, a DES-based robot-motion-mode control and application of the Artificial Potential Field model for ensuring collision-free motion of two robots sharing a space sector. Next we assume simple robot control and subject the system to simulation experiments aimed at comparing the impact of the different solutions on the performance of MMRS.
- **Mixed Nondeterministic-Probabilistic Automata**

Authors: Albert Benveniste ; Jean-Baptiste Raclet
Abstract: Graphical models in probability and statistics are a core concept in the area of probabilistic reasoning and probabilistic programminggraphical models include Bayesian networks and factor graphs. For modeling and formal verification of probabilistic systems, probabilistic automata were introduced. This paper proposes a coherent suite of models consisting of Mixed Systems, Mixed Bayesian Networks, and Mixed Automata, which extend factor graphs, Bayesian networks, and probabilistic automata with the handling of nondeterminism. Each of these models comes with a parallel composition, and we establish clear relations between these three models. Also, we provide a detailed comparison between Mixed Automata and Probabilistic Automata

- **Correction to: Local and global robustness with q-step delay for max-plus linear systems**
Authors: Yingxuan Yin ; Yuegang Tao ; Cailu Wang ; Haiyong Chen
Correction to: Discrete Event Dynamic Systems (2021) 32:231-251 The second sentence ("Currently, she is a associate professor ") in the biography of Author Cailu Wang in the above reference article is to be replaced by as follows: "Currently, she is a post-doctor at the School of Automation, Beijing Institute of Technology." The author Cailu Wang regrets an incorrect information for her institution being published in the above reference article. The correct institution is "School of Automation, Beijing Institute of Technology, Beijing 100081, Peoples Republic of China".

- **Correction to: Transformational supervisor synthesis for evolving systems**
Authors: Sander Thuijsman ; Michel Reniers
Abstract: The paper mentioned in the title used an incorrect implementation of the algorithms to produce the experimental results. The mistake significantly impacts the computational efficiency of the algorithms, on which they are evaluated. In this correction we explain the mistake, present the new results, and update our conclusions based on the new results.

Back to the contents

1.2. IEEE Transactions on Automatic Control
Volume: 68, Issue: 12, December 2023

- **Hierarchical Supervisory Control Under Partial Observation: Normality**
Authors: Jan Komenda ; Tomá Masopust
Abstract: Conditions preserving observability of specifications between the plant and its abstraction are essential for hierarchical supervisory control of discrete-event systems under partial observation. Observation consistency and local observation consistency were identified as such conditions. To preserve normality, only observation consistency is required. Although observation consistency preserves normality between the levels for normal specifications, for specifications that are not normal, observation consistency is insufficient to guarantee that the supremal normal sublanguage computed on the low level and on the high level coincide. We define modified observation consistency, under which the supremal normal sublanguages of different levels coincide. We show that the verification of (modified) observation consistency is PSpace -hard for finite automata and undecidable for slightly more expressive models than finite automata. Decidability of (modified) observation consistency is an open problem. Hence we further discuss two stronger conditions that are easy to verify. Finally, we illustrate the conditions on an example of a railroad controller and on a case study of a part of an MRI scanner.

- **Multiagent, Multitarget Path Planning in Markov Decision Processes**
Authors: Farhad Nawaz ; Melkior Ornik
Abstract: Missions for autonomous systems often require agents to visit multiple targets in complex operating conditions. This work considers the problem of visiting a set of targets in minimum time by a team of noncommunicating agents in a Markov decision process (MDP). The single-agent problem is at least NP-complete by reducing it to a Hamiltonian path problem. We first discuss an optimal algorithm based on Bellman's optimality equation that is exponential in the number of target states. Then, we tradeoff optimality for time complexity by presenting a suboptimal algorithm

that is polynomial at each time step. We prove that the proposed algorithm generates optimal policies for certain classes of MDPs. Extending our procedure to the multiagent case, we propose a target partitioning algorithm that approximately minimizes the expected time to visit the targets. We prove that our algorithm generates optimal partitions for clustered target scenarios. We present the performance of our algorithms on random MDPs and gridworld environments inspired by ocean dynamics. We show that our algorithms are much faster than the optimal procedure and more optimal than the currently available heuristic.

- **Probabilistic Safety Guarantees for Markov Decision Processes**
  Authors: Rafal Wisniewski ; Manuela L. Bujorianu
  Abstract: This article aims to incorporate safety specifications into Markov decision processes. Explicitly, we address the minimization problem up to a stopping time with safety constraints. We establish a formalism leaning upon the evolution equation to achieve our goal. We show how to compute the safety function with dynamic programming. In the last part of this article, we develop several algorithms for safe stochastic optimization using linear and dynamic programming.

- **Critical Observability Verification and Enforcement of Labeled Petri Nets by Using Basis Markings**
  Authors: Xuya Cong ; Maria Pia Fanti ; Agostino Marcello Mangini ; Zhiwu Li
  Abstract: A discrete event system is said to be critically observable if the observer can always determine whether the current state necessarily belongs to a set of critical states. This article focuses on two issues related to the safety and security of discrete event systems, namely critical observability verification and enforcement of labeled Petri nets. First, given a bounded net, we verify its critical observability by using basis markings and solving some integer linear programming problems, thus avoiding the enumeration of the full state space of a net system. Moreover, for a noncritically observable net system, we obtain a feasible stop-free event set from a twin basis reachability graph such that a valid control policy can always be found, if the feasible stop-free event set is nonempty. Finally, according to the feasible stop-free event set, a set of disabled edges is generated, and an online control policy is developed based on the supervisory control theory, which guarantees that the closed-loop system is critically observable and deadlock free.

- **Observability and Detectability of Stochastic Labeled Graphs**
  Authors: Shiyong Zhu ; Jinde Cao ; Lin Lin ; Leszek Rutkowski ; Jianquan Lu ; Guoping Lu
  Abstract: In this article, observable stochastic graphs and detetectable stochastic graphs are, respectively, defined with the detailed implementation for the observability and detectability of stochastic discrete-time and discrete-state dynamic systems. More specifically, they are generally two classes of vertex-colored and edge-labeled graphs rendering a walking agent therein to determine his initial and current positions, respectively, in probability one by measuring the color sequence of his traversed vertices. In the part of analysis, we follow the aforementioned two definitions and establish the corresponding polynomial-time verifying algorithms. Notably, the implicit formulas are also established to calculate the observability and detectability probability for any pairwise vertex pair. In the synthesis part, the minimal number of colors dyeing the vertices to make the considered graph stochastically observable and detectable is investigated, respectively. Our results indicate that the minimal coloring problem is NP-hard for observability in the stochastic situations but is solvable in polynomial time for detectability in the deterministic cases. The observability and detectability of stochastic finite-valued systems, assembling with the finite-cardinal state spaces, are validated as a compelling application of these two types of directed graphs, whereas the minimal sensors placement problems subject to observability and detectability problems are accordingly interpreted by the minimum set cover algorithm.

- **Algebraic Reduction of Hidden Markov Models**
  Authors: Tommaso Grigoletto ; Francesco Ticozzi
  Abstract: The problem of reducing a hidden Markov model (HMM) to one of smaller dimension that exactly reproduces the same marginals is tackled by using a system-theoretic approach. Realization theory tools are extended to HMMs by leveraging suitable algebraic representations of probability spaces. We propose two algorithms that return coarse-grained equivalent HMMs obtained by stochastic projection operators: the first returns models that exactly reproduce the

single-time distribution of a given output process, while in the second, the full (multitime) distribution is preserved. The reduction method exploits not only the structure of the observed output but also its initial condition, whenever the latter is known or belongs to a given subclass. Optimal algorithms are derived for a class of HMMs, namely observable ones.

- **Continuous-Observation One-Sided Two-Player Zero-Sum Partially Observable Stochastic Game With Public Actions**
  Authors: Wei Zheng ; Taeho Jung ; Hai Lin
  Abstract: The one-sided two-player zero-sum partially observable stochastic games (OTZ-POSG) have emerged as popular models recently, especially in the cyber-security literature. In this game, the state is hidden for one player but directly observed by the other player for whom we call the informed player. All existing OTZ-POSG models assumed that the observation space is discrete and the action of the informed player is private. However, these assumptions may become invalid in real applications. For example, for the virtual machine migration techniques in moving target defenses, the observed traffic data of a network are in a continuous space and the switching strategy of the defender can be inferred by the attacker. This article, therefore, proposes a continuous-observation OTZ-POSG with public actions and studies the existence of its equilibrium. The main challenge induced by the public action is the potential information leakagethe action of the informed player could reveal state information because his or her policy is state dependent. To solve this issue, we adopt a two-step belief update strategy for players and prove the existence of a Stackelberg equilibrium. We show that the game can be solved iteratively through value iteration. However, calculating the exact value function is impractical as the observation space is continuous. To mitigate the computational complexity issue, we propose a point-based approximation algorithm to approximate the exact value function and meanwhile extend the dynamic partitioning approach to discretize the observation space into finite discrete partitions. We show that the value function of the leader can be approximated by a piece-wise linear and concave function with an error bound. Finally, examples are used in each section to illustrate ideas of the proposed algorithms.

Back to the contents

1.3. Automatica

Volume: 158, December 2023

- **Optimal transmission strategy for multiple Markovian fading channels: Existence, structure, and approximation**
  Authors: Yong Xu ; Haoxiang Xiang ; Lixin Yang ; Renquan Lu ; Daniel E. Quevedo
  Abstract: This paper investigates the optimal transmission strategy for remote state estimation over multiple Markovian fading channels. A smart sensor is used to obtain a local state estimate of a system, and transmits it to a remote estimator. A new transmission strategy is proposed by co-designing the channel allocation and the transmission power control. The co-designing problem is modeled as a constrained Markov decision process (CMDP) to minimize the expected average estimation error covariance subject to the energy constraint over an infinite horizon. The CMDP is then relaxed as an unconstrained Markov decision process (UMDP) using the Lagrange multiplier method. Sufficient conditions for the existence of the optimal stationary policy for the UMDP are established to obtain the optimal transmission strategy. The structure of the optimal transmission power control policy for the UMDP with discounted cost is also elucidated. Taking account of the discrete-continuous hybrid action space, a parameterized deep Q-network (P-DQN) algorithm is employed to obtain an approximate optimal policy for the UMDP. Finally, a moving vehicle example is introduced to illustrate the effectiveness of the developed methods.
- **Dynamic event-triggered adaptive control for a class of uncertain nonlinear systems**
  Authors: Lantao Xing ; Changyun Wen
  Abstract: This paper investigates the event-triggered control problem for a class of strict-feedback uncertain nonlinear systems. For such kind of systems, many backstepping-based event-triggered control methods have been proposed. However, these currently available methods all adopt static event conditions which cannot simultaneously guarantee zero tracking/stabilization error and non-existence of the Zeno behavior. In this paper, a dynamic event-triggered control scheme for strict-feedback uncertain nonlinear systems is proposed. In this scheme, an auxiliary dynamic variable

is included in the event condition. By properly designing the dynamics of this auxiliary variable, the proposed dynamic event-triggered control scheme can ensure zero tracking/stabilization error in the absence of Zeno behavior. Simulation results are provided to illustrate the effectiveness of the proposed scheme and verify the established theoretical results.

- **Unbiased minimum-variance estimation and dynamic event-driven disturbance rejection control for discrete time-varying systems**
  Authors: Jinhui Zhang ; Hao Xu ; Jianfang Yin
  Abstract: This paper studies a dynamic event-driven disturbance rejection control problem for a class of linear discrete time-varying systems with unknown external disturbances, random process and measurement noises. To obtain the accurate estimates of both the system states and external disturbances, simultaneously, an unbiased minimum-variance time-varying extended state observer is designed, and the stability of the estimation error system is analyzed. Then, a dynamic event-driven disturbance rejection controller is designed by minimizing the upper bound of the cost function of the closed-loop system over a finite horizon. It can be shown that, by applying the proposed control approach, not only the transmission frequency of the control signal is reduced, but also the external disturbances are compensated actively. Finally, numerical simulations are given to demonstrate the effectiveness of the proposed control approaches.

Back to the contents

1.4. IEEE Control Systems Letter

Volume: 7, Issue:11, November 2022

- **Data-Driven Controller Synthesis via Finite Abstractions With Formal Guarantees**
  Authors: Daniel Ajeleye ; Abolfazl Lavaei ; Majid Zamani
  Abstract: Construction of finite-state abstractions (a.k.a. symbolic abstractions) is a promising approach for formal verification and controller synthesis of complex systems. Finite-state abstractions provide simpler models that can replicate the behaviors of original complex systems. These abstractions are usually constructed by leveraging precise knowledge of systems dynamics, which is often unknown in real-life applications. In this letter, we develop a data-driven technique for constructing finite abstractions for continuous-time control systems with unknown dynamics. In our data-driven context, we collect samples from trajectories of unknown systems to construct finite abstractions with a guarantee of correctness. We propose a data-based gridding method to efficiently determine state-set discretization parameters while minimizing the expected number of transitions in the abstraction construction, thus reducing computational efforts. By establishing a feedback refinement relationship between an unknown system and its data-driven finite abstraction, one can design a controller over the data-driven finite abstraction. The controller can then be refined back to the original unknown system to meet a desired property of interest. We illustrate our proposed data-driven approach using a vehicle motion planning benchmark.
- **A Consensus Q-Learning Approach for Decentralized Control of Shared Energy Storage**
  Authors: Amit Joshi ; Massimo Tipaldi ; Luigi Glielmo
  Abstract: In this letter, we study the say decentralized scheduling of an energy storage system say shared among residential households. In particular, we consider the households as learning agents and model their interaction as a Markov Game. To address the challenges associated with the non-stationary nature of the multi-agent learning, we propose a consensus-based Tabular Q-learning method. Additionally, we provide simulation studies utilizing a real-world household dataset and demonstrate the effectiveness of our approach.

Back to the contents

1.5. Control Engineering Practice

Volume: 141, December 2023

- **A protocol for Decentralized Synchronous Diagnosis with Coordination**
  Authors: Patricia C. Mayer ; Felipe G. Cabral ; Marcos V. Moreira

Abstract: Recently, a new architecture for decentralized diagnosis of Discrete Event Systems, called Decentralized Synchronous Diagnosis, has been proposed in the literature. In this scheme, local diagnosers are computed based on the fault-free behavior of the system components, which, in comparison with the classical diagnosis approach, reduces the size of local diagnosers for implementation. Although this method has been successfully implemented, its main drawback is the emergence of an exceeding fault-free language of the system for diagnosis, which reduces the diagnosis efficiency. To circumvent this problem, in this paper, a protocol for Decentralized Synchronous Diagnosis with Coordination (DSDC), which refines the diagnosis status using cluster automata of the local component models, is proposed. The protocol is based on the implementation of local state estimators of the fault-free component models of the system which communicate cluster automata to a coordinator. The indication of the fault occurrence is carried out by the coordinator according to the observed behavior of the system. To do so, communication rules between local state estimators and the coordinator are proposed. The protocol prevents the emergence of an exceeding fault-free language for diagnosis, which guarantees the same diagnosis performance as the traditional monolithic approach. In addition, the implementation of the DSDC in a didactic manufacturing system is presented to illustrate the results.

Back to the contents

1.6. International Journal of Control

Volume: 96, Issue: 12, December 2023

- **Least-cost transition sequence estimation in labelled time Petri net systems with unobservable transitions**

  Authors: Liang Li ; Yaqiong Li ; Bin Liu ; and Weimin Wu

  Abstract: This paper presents an approach to solve the least-cost transition sequences estimation problem in labelled time Petri net (LTPN) systems with unobservable transitions. Particularly, the considered LTPN system is bounded, in which each transition has a nonnegative cost and is labelled as either observable or unobservable. We first introduce a graph, called a segmented modified state class graph (SMSCG), that is a compact representation of the partial state space of an LTPN system. Based on the SMSCG and an observed time-label sequence, a method to estimate logic consistent transition sequences is proposed. By exploiting the transitions-related timing constraints in SMSCGs, a procedure for determining which logic consistent transition sequences are timing consistent with the observed time-label sequence and a given time is reported. Finally, we develop an algorithm to perform the estimation of least-cost transition sequences.

Back to the contents

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

Volume: 53, Issue: 12, December 2023

- **Modeling and Analyzing Logic Vulnerabilities of E-Commerce Systems at the Design Phase**

  Authors: Wangyang Yu ; Lu Liu ; Xiaoming Wang ; Ovidiu Bagdasar ; John Panneerselvam

  Abstract: E-commerce systems have become tremendously popular and important for modern business processes in the world of the digital economy. E-commerce business processes rely on the distributed and concurrent interaction process among Web applications of participants, such as clients, merchants, third-party payment platforms (TPPs), and bank systems. Such complex business interactions bridge the gap of trustiness among participants and introduce new security challenges in the form of logical vulnerabilities, which are prevalent in the business process at the application level. The most pressing challenge is to guarantee security throughout the checkout process at the conceptual design phase such that the logic errors can be detected before the actual implementation. Maintenance and repair of implemented e-commerce systems can be extremely costly. To this end, this article proposes a novel modeling and analyzing methodology for multiparticipants and multisessions e-commerce interaction processes based on colored Petri nets (CPNs). First, we define a novel model that can efficiently depict the key properties of e-commerce busi-

ness interaction processes. Second, several modeling principles are formulated based on the design specification of e-commerce systems. Finally, the concept of Transaction-Logical Consistency is defined to analyze and verify the logical vulnerabilities of e-commerce systems. Through a discussed case study, we demonstrate the feasibility and applicability of the proposed methodology and its efficiency in detecting problems those can potentially lead to logical vulnerabilities.

Back to the contents

2 Call for Participants

2.1 EECI-IGSC Course: Introduction to Discrete Event Systems

Dear Colleagues,

We would like to draw your attention to the course titled "**Introduction to Discrete Event Systems**", to be taught by **Christos Cassandras** (Boston University, USA) and **Stéphane Lafortune** (University of Michigan, USA), which will be held from **June 3 to June 7, 2024, at the Campus Saint Charles, in Marseille, France**. Isabel Demongodin is the local organizer.

This course of 21 hours, offered as part of the European Embedded Control Institute-International Graduate School on Control (M13 of EECI-IGSC-2024), is especially designed for doctoral students, post-docs and junior researchers, who will have the opportunity to learn the main concepts and recent results in the theory and application of discrete event systems.

While the area of discrete event systems started as a sub-discipline in control engineering almost 40 years ago, the study of discrete event systems (DES) remains highly relevant to control engineering problems nowadays, such as in cyber-physical systems, transportation, software engineering, and in the study of privacy and security in engineered systems. In fact, DES form the centerpiece of the event-driven (cyber) component in the hybrid systems that comprise much of todays technology, complementing the time-driven (physical) components.

This course will strike a balance between introducing the students to the key concepts, models, and results of discrete-event control theory for logical and stochastic models, while at the same time emphasizing current research trends in DES theory and applications.

Please see the EECI's webpage, http://www.eeci-igsc.eu/, for further details.

Students can apply to get financial support. Pour les doctorants inscrits dans une Université française hors Ile-de-France, voir : http://www.eeci-igsc.eu/igsc-grant-registration-france/. For Female PhD Students PhD Students from countries with Low Education Priorities, see http://www.eeci-igsc.eu/igsc-grant-registration-overseas/.

The registration is open as "M13-MARSEILLE-03/06/2024-07/06/2024" at: http://www.eeci-igsc.eu/earlyregistrationm03tom18/. While the early registration deadline is April 1, 2024, please register as "Administration fee" (20) as soon as possible and by February 15, 2024, to ensure participation.

Looking forward to seeing many of you in Marseille next year!

Best regards,

Isabel Demongodin, Christos Cassandras and Stéphane Lafortune

2.2 Workshop at CDC'23 Singapore: Formal Methods in System Resilience: From Analysis to Control

Dear colleagues,

We would like to bring your attention to the workshop on the topic of **"Formal Methods in System Resilience: From Analysis to Control" at IEEE CDC 2023, to take place in Singapore, December 12, 2013**, organized by Rong Su (Nanyang Technological University), and Xiang Yin (Shanghai Jiao Tong University).

The workshop will feature invited talks from Alessandro Abate (University of Oxford), Alessandro Giua (University of Cagliari), Christoforos Hadjicostis (University of Cyprus), Zhiwu Li (Macau University of Science and Technology), Rong Su (Nanyang Technological University), Xiang Yin (Shanghai Jiao Tong University), and Majid Zamani (University of Colorado, Boulder); as well as a panel discussion.

For more details on the talks will be updated at https://sites.google.com/view/cdc23workshop.

Registration information of the workshop can be found at https://cdc2023.ieeecss.org/registration.

2.3 Invited Session at WODES'24–Resilience and Security of Discrete Event Systems

Organizer

- Romulo Meira-Goes, Assistant Professor, Penn State University, romulo@psu.edu
- Ilya Kovalenko, Assistant Professor, Penn State University, iqk5135@psu.edu
- Xiang Yin, Associate Professor, Shanghai Jiao Tong University, yinxiang@sjtu.edu.cn

Summary Statement

Driven by the needs of many different application domains, the field of Discrete Event Systems (DESs) has shown success in modeling and analyzing complex systems. In DES, the operation of systems is modeled in an event-based manner and only important details are considered in analyzing their operation. Recently, the field of DES has been used in engineering systems that combine physical processes controlled by computational infrastructures, denoted as Cyber-Physical Systems (CPS). The methods developed in DES were shown to help provide the necessary safety, security, and resilience guarantees for CPS. However, the ever-increasing demands for these properties in critical CPS put stringent constraints on their analysis and design. This invited session aims to tackle these challenges for the important class of CPS that can be modeled by DESs. This class of CPS includes applications in the areas of manufacturing systems, transportation systems, chemical systems, software engineering, etc.

The main objective for this invited session is to gather recently developed novel approaches devoted to the analysis, design, and enforcement of security and resilience properties using DES models. We seek submissions including but not limited to the following topics:

- Modeling and analysis of cyber-security of DES
- Applications of DES-based modeling and control for CPS resilience and security
- Analysis and design of DES under cyber-attacks
- Supervisory control and fault-tolerant control of networked DES
- Opacity, diagnosability, observability analysis of DES

Submission Code: 3afg1

Back to the contents

3 Conferences

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

3.1 **2023 IEEE Conference on Decision and Control (CDC)**
Singapore, December 13-15, 2023.
https://cdc2023.ieeecss.org/

3.2 **2024 IFAC Workshop on Discrete Event Systems (WODES)**
Rio de Janeiro, Brazil, April 29-May 1, 2024.
https://wodes2024.eventos.ufrj.br

3.3 **2024 IFAC Conference on Analysis and Design of Hybrid Systems (ADHS)**
Boulder, Colorado, July 1-3, 2024.
https://www.colorado.edu/conference/adhs2024/

3.4 **2024 American Control Conference (ACC)**
Toronto, Canada, July 8-12, 2024.
https://acc2024.a2c2.org/

3.5 **2024 International Conference on Automation Science and Engineering (CASE)**
Bari, Italy, August 28-September 1, 2024.
https://2024.ieeecase.org/

Back to the contents

4 Books

4.1 Safe Autonomy with Control Barrier Functions: Theory and Applications

Authors: Wei Xiao, Christos G. Cassandras, and Calin Belta

Description: The book presents the concept of Control Barrier Function (CBF), which captures the evolution of safety requirements during the execution of a system and can be used to enforce safety. Safety is central to autonomous systems since they are intended to operate with minimal or no human supervision. The book includes both theoretical and application perspectives on how safety can be guaranteed. It explains how the CBF approach is computationally efficient and can easily deal with nonlinear models and complex constraints used in a wide spectrum of applications, including autonomous driving, robotics, and traffic control. Safety guarantees can be integrated into the operation of such autonomous systems, including typical safety requirements that involve collision avoidance, technological system limitations, and bounds on real-time executions. Adaptive and event-driven approaches for safety are also discussed for time-varying execution bounds and noisy dynamics, as well as for systems with unknown dynamics.

Additional information on the book can be found at
https://link.springer.com/book/10.1007/978-3-031-27576-0
where an eBook version can also be downloaded (free for some educational institutions).

4.2 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

4.3 Introduction to Discrete Event Systems (Third Edition)

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

4.4 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

5 Software Tools

5.1 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.

5.2 Eclipse ESCET™ version 1.0 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 2023, ESCET version 1.0 has been released and can be downloaded from https://www.eclipse.org/escet/download.html. The main changes in this version are

- The Eclipse ESCET project has graduated. The project has left the 'incubation' phase, and has entered the 'mature' phase. In honor of this occasion, we leave the '0.x' version numbering behind. All indications of the incubation phase have been removed. This also leads to changes in download filenames.
- The CIF language now features annotations that can be used to annotate elements of the specification with extra information. The CIF toolset now comes bundled with the doc annotation. Annotations are currently an experimental work-in-progress language feature. Their design may change in a backward incompatible manner.
- The CIF controller checker had a performance regression since version 0.7 in case finite response is checked and confluence is not checked. This performance regression has been fixed.
- The CIF to Supremica transformation now correctly transforms multiple guards on an edge. Multiple guards are now combined into a single conjunction.
- The CIF data-based synthesis tools workset algorithm now has improved edge selection heuristics, improving the performance of the workset algorithm. Its documentation has been improved to better explain when to use and not to use the workset algorithm. Also, the workset algorithm is no longer considered experimental.

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.

5.3 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.

5.4 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.

5.5 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.

5.6 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