IEEE Control Systems Society
Technical Committee on Discrete Event Systems

Newsletter **November 2024**

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 2024 November 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. IEEE Transactions on Automatic Control

Volume: 69, Issue: 11, November 2024

- **Enforcement of Current-State Opacity in Signal Interpreted Petri Nets**
  Authors: Andreas Köhler ; Pascal Marijan ; Ping Zhang
  Abstract: This article proposes a new approach for the enforcement of current-state opacity in signal interpreted Petri nets (SIPN). In order to enforce current-state opacity in SIPNs, the properties of iterative firing and simultaneous firing of transitions are considered. To prevent the intruder from inferring the current marking, signals associated with the secret marking are compared to signals associated with alternative markings. This allows to determine which signals need to be encrypted to confuse the secret marking with markings leading to the secret marking, markings directly reachable from the secret marking or markings reachable from the premarking of the secret marking. The proposed approach applies to any system that can be described by an SIPN.
- **Nonexistence of Upper Bound to Inferencing Level in Decentralized Discrete Event Control**
  Authors: Shigemasa Takai ; Ratnesh Kumar
  Abstract: In the authors' earlier work, the notion of inference-observability was introduced to characterize the existence of decentralized supervisors that perform multilevel inferencing against self-ambiguity and the ambiguities of others to jointly arrive at a correct control decision. When the property of N -inference-observability holds, N-levels of inferencing are needed. We show in this article that the class of N-inference-observable languages increases strictly monotonically as the parameter N is increased. We further show that, in general, there is no upper bound on the number of levels of inferencing required.
- **On the Existence of Nonblocking Bounded Supervisors for Discrete-Event Systems**
  Authors: Zhaoyu Xiang ; Yufeng Chen ; Naiqi Wu ; Zhiwu Li
  Abstract: This article investigates the supervisory control problem of discrete-event systems modeled with deterministic finite-state automata. Given a control specification represented by a nonempty regular sublanguage of the generated language of a plant, we aim to solve a synthesis problem for finding a nonblocking supervisor for the control specification to guarantee that there exists an integer such that the length of any string in the generated language of the plant under supervision is no greater than the integer, namely a bounded nonblocking supervisor. We show that the problem can be reduced to finding a positional winning strategy in a two-player reachability game. Examples are presented to illustrate the reported approach.
- **Zonotope-Based Symbolic Controller Synthesis for Linear Temporal Logic Specifications**
  Authors: Wei Ren ; Raphaël M. Jungers ; Dimos V. Dimarogonas
  Abstract: This article studies the controller synthesis problem for nonlinear control systems under linear temporal logic (LTL) specifications using zonotope techniques. A local-to-global control strategy is proposed for the desired specification expressed as an LTL formula. First, a novel approach is developed to divide the state space into finite zonotopes and constrained zonotopes, which are called cells and allowed to intersect with the neighbor cells. Second, from the intersection relation, a graph among all cells is generated to verify the realization of the accepting path for the LTL formula. The realization verification determines if there is a need for the control design, and also results in finite local LTL formulas. Third, once the accepting path is realized, a novel abstraction-based method is derived for the controller design. In particular, we only focus on the cells from the realization verification and approximate each cell thanks to properties of zonotopes. Based on local symbolic models and local LTL formulas, an iterative synthesis algorithm is proposed to design all local abstract controllers, whose existence and combination establish the global controller for the LTL formula. Finally, the proposed framework is illustrated via a path planning problem of mobile robots.

- **Scalable Synthesis of Safety Barrier Certificates for Networks of Stochastic Switched Systems**
  Authors: Abolfazl Lavaein ; Emilio Frazzoli
  Abstract: In this article, we propose a compositional scheme for the safety controller synthesis of stochastic switched networks with dwell-time conditions. The proposed framework is based on a notion of so-called transition subbarrier certificates constructed for each switched subsystem, by employing which one can compositionally synthesize safety controllers for interconnected networks over (in)finite time horizons. In our proposed scheme, we leverage dissipativity-type compositional conditions to compositionally construct transition barrier certificates for interconnected networks based on their corresponding subbarrier certificates of individual subsystems. We show that the provided compositionality conditions can utilize the structure of the interconnection topology and be potentially satisfied independently of the number or gains of subsystems. We then utilize the constructed transition barrier certificates and quantify upper bounds on the probability that the interconnected network reaches certain unsafe regions in (in)finite time horizons. For nonlinear stochastic systems with polynomial dynamics, we employ sum-of-squares (SOS) optimization programs to search for stochastic storage certificates of each switching mode with its independent supply rate . We then focus on a particular class of nonlinear stochastic switched systems whose nonlinearities satisfy some linear-growth restriction and propose a constructive approach to search for storage certificates of each mode via satisfying some matrix inequalities. We demonstrate our proposed results by applying them to a fully interconnected network of 400 nonlinear switched subsystems (totally 800 dimensions) accepting multiple supply rates and multiple storage certificates with dwell-time conditions.
- **Data-Driven Control of Unknown Switched Linear Systems Using Scenario Optimization**
  Authors: Zheming Wang ; Guillaume O. Berger ; Raphaël M. Jungers
  Abstract: We tackle uniform state feedback control of switched linear systems under arbitrary switching using scenario optimization. We propose a data-driven control framework, in which scenario programs are formulated to compute stabilizing state feedback control relying on a finite set of observations of trajectories with quadratic and sum of squares (SOS) Lyapunov functions. We do not require the exact dynamical model or the switching signal, and as a consequence, we aim at solving uniform stabilization problems, in which the feedback is stabilizing for all possible switching sequences. In order to generalize the solution obtained from trajectories to the actual system, probabilistic guarantees on the obtained quadratic or SOS Lyapunov function are derived in the spirit of scenario optimization. For the quadratic Lyapunov technique, the generalization relies on a geometric analysis argument, while, for the SOS Lyapunov technique, we follow a sensitivity analysis argument. In order to deal with high-dimensional systems, we also develop a parallelized scheme for the proposed approach. We show that, with some modifications, the data-driven quadratic Lyapunov technique can be extended to linear quadratic regulator (LQR) control design. Finally, the proposed data-driven control framework is demonstrated on several numerical examples.
- **Learning Optimal Strategies for Temporal Tasks in Stochastic Games**
  Authors: Alper Kamil Bozkurt ; Yu Wang ; Michael M. Zavlanos ; Miroslav Pajic
  Abstract: Synthesis from linear temporal logic (LTL) specifications provides assured controllers for systems operating in stochastic and potentially adversarial environments. Automatic synthesis tools, however, require a model of the environment to construct controllers. In this work, we introduce a model-free reinforcement learning (RL) approach to derive controllers from given LTL specifications even when the environment is completely unknown. We model the problem as a stochastic game (SG) between the controller and the environment; we then learn optimal strategies that maximize the probability of satisfying the LTL specifications against the worst-case environment behavior. We first construct a product game using the deterministic parity automaton (DPA) translated from the given LTL specification. By deriving distinct rewards and discount factors from the acceptance condition of the DPA, we reduce the maximization of the worst-case probability of satisfying the LTL specification into the maximization of a discounted reward objective in the product game; this enables the use of model-free RL algorithms to learn an optimal controller strategy.

To address the scalability issues arising when the number of sets defining the acceptance condition of the DPA, usually referred to as colors, is large; we propose a lazy color generation method where distinct rewards and discount factors are utilized only when needed, and an approximate method where the controller eventually focuses on only one color. In several case studies, we show that our approach is scalable to a wide range of LTL formulas, significantly outperforming existing methods that learn controllers from LTL specifications in SGs.

Back to the contents

1.2. Automatica

Volume: 169, November 2024

- **Stability and bounded real lemmas of discrete-time MJLSs with the Markov chain on a Borel space**
  Authors: Chunjie Xiao ; Ting Hou ; Weihai Zhang
  Abstract: In this paper, exponential stability of discrete-time Markov jump linear systems (MJLSs) with the Markov chain on a Borel space $(\Theta, \mathcal{B}(\Theta))$ is studied, and bounded real lemmas (BRLs) are given. The work generalizes the results from the previous literature that considered only the Markov chain taking values in a countable set to the scenario of an uncountable set and provides unified approaches for describing exponential stability and H_∞ performance of MJLSs. This paper covers two kinds of exponential stabilities: one is exponential mean-square stability with conditioning (EMSSy-C), and the other is exponential mean-square stability (EMSSy). First, based on the infinite-dimensional operator theory, the equivalent conditions for determining these two kinds of stabilities are shown respectively by the exponentially stable evolutions generated by the corresponding bounded linear operators on different Banach spaces, which turn out to present the spectral criteria of EMSSy-C and EMSSy. Furthermore, the relationship between these two kinds of stabilities is discussed. Moreover, some easier-to-check criteria are established for EMSSy-C of MJLSs in terms of the existence of uniformly positive definite solutions of Lyapunov-type equations or inequalities. In addition, BRLs are given separately in terms of the existence of solutions of the Θ-coupled difference Riccati equation for the finite horizon case and algebraic Riccati equation for the infinite horizon case, which facilitates the H_∞ analysis of MJLSs with the Markov chain on a Borel space.
- **Adaptive generalized Nash equilibrium seeking algorithm for nonsmooth aggregative game under dynamic event-triggered mechanism**
  Authors: Mengxin Wang ; Jianing Chen ; Changyun Wen ; Sitian Qin
  Abstract: This paper addresses a nonsmooth aggregative game to control multiple noncooperative players, each with a nonsmooth cost function that depends not only on its own decision but also on some aggregate effect among all the agents. In addition, the decision of each player is restricted by private and coupling constraints. To address these concerns, a distributed generalized Nash equilibrium (GNE) seeking algorithm is proposed. Two features distinguish our methods from the existing GNE seeking algorithms. Firstly, an adaptive penalty method is introduced to drive each player's action to enter the set of private constraints. The adaptive term ensures automatic adjustment of penalty parameter based on the degree of constraint violation excluding any prior calculation. Secondly, a distributed dynamic event-triggered mechanism is designed for each player to lessen communication energy. In comparison to the static event-triggered mechanism, the proposed dynamic mechanism possesses larger inter-execution time intervals. As the discontinuity of the event-triggered mechanism can impact the existence of a solution to the closed-loop system in the classical sense, we adapt a nonsmooth analysis technique, including differential inclusion and Filippov solution. Through nonsmooth Lyapunov analysis, the convergence result and the avoidance of Zeno behavior are established. Finally, two engineering examples are provided to demonstrate the validity of the theoretical results.
- **Compositional synthesis for linear systems via convex optimization of assume-guarantee contracts**
  Authors: Kasra Ghasemi ; Sadra Sadraddini ; Calin Belta
  Abstract: We take a divide and conquer approach to design controllers for reachability problems given large-scale linear systems with polyhedral constraints on states, controls, and disturbances.

Such systems are made of small subsystems with coupled dynamics. We treat the couplings as additional disturbances and use assume-guarantee (AG) contracts to characterize these disturbance sets. For each subsystem, we design and implement a robust controller locally, subject to its own constraints and contracts. The main contribution of this paper is a method to derive the contracts via a novel parameterization and a corresponding potential function that characterizes the distance to the correct composition of controllers and contracts, where all contracts are held. We show that the potential function is convex in the contract parameters. This enables the subsystems to negotiate the contracts with the gradient information from the dual of their local synthesis optimization problems in a distributed way, facilitating compositional control synthesis that scales to large systems. We present numerical examples, including a scalability study on a system with tens of thousands of dimensions, and a simple case study on applying our method to a distributed Model Predictive Control (MPC) problem in a power system.

Back to the contents

1.3. IEEE Control Systems Letter

Volume: 8, Issue: 10, November 2024

- **Computation and Formal Verification of Neural Network Contraction Metrics**
  Authors: Maxwell Fitzsimmons ; Jun Liu
  Abstract: A contraction metric defines a differential Lyapunov-like function that robustly captures the convergence between trajectories. In this letter, we investigate the use of neural networks for computing verifiable contraction metrics. We first prove the existence of a smooth neural network contraction metric within the domain of attraction of an exponentially stable equilibrium point. We then focus on the computation of a neural network contraction metric over a compact invariant set within the domain of attraction certified by a physics-informed neural network Lyapunov function. We consider both partial differential inequality (PDI) and equation (PDE) losses for computation. We show that sufficiently accurate neural approximate solutions to the PDI and PDE are guaranteed to be a contraction metric under mild technical assumptions. We rigorously verify the computed neural network contraction metric using a satisfiability modulo theories solver. Through numerical examples, we demonstrate that the proposed approach outperforms traditional semidefinite programming methods for finding sum-of-squares polynomial contraction metrics.

Back to the contents

1.4. IEEE Transactions on Control Systems Technology

Volume: 32, Issue: 6, November 2024

- **Enhanced Optimal Symbolic Controller Synthesis: Application to a Boiler System**
  Authors: Alireza Najafiyanfar ; Babak Tavassoli
  Abstract: Reliable and provably correct performance of control systems in the presence of various types of uncertainties and disturbances are essential objectives that require high integrity of the whole control system. Symbolic control is a candidate method for achieving these objectives which is capable of addressing both robustness and optimality of controller. However, several challenges may arise when the symbolic control method is applied in practice. These include the load of design computations, high memory requirements for design and implementation, and oscillations caused by discretization of inputs. The focus of this work is on treatment of the mentioned challenges during symbolic control synthesis for a boiler system as the central safety critical element in a broad range of industries. To reduce the load of design computations and the required memory while preserving the control precision, a two-stage control scheme is used in which symbolic models with different resolutions are employed. The input oscillations are also reduced by minimizing the changes in the input at the steady state. The performance of the synthesized controllers for several different designs are evaluated and compared during a simulation study. The results demonstrate the suitable performance of the symbolic control method when applied to a boiler system.

Back to the contents

1.5. IEEE Transactions on Automation Science and Engineering

Volume: 21, Issue: 4, November 2024

- **A Digital Twin Approach for Enforcing Diagnosability in Petri Nets**
  Authors: Shaopeng Hu ; Zhiwu Li
  Abstract: This paper addresses the problem of fault diagnosis and diagnosability enforcement of discrete event systems. Given a nondiagnosable discrete event system modeled with Petri nets, which may enter deadlocks and unobservable live-locks, a digital twin system (derived from the original Petri net model) can be established as a particular Petri net such that the closed-loop system established from the original system under the control of its digital twin counterpart is diagnosable. This procedure employs a deterministic finite automaton (derived from the digital twin system) to diagnose the closed-loop system and provides necessary and sufficient conditions for diagnosability enforcement. In this way, we do not need to compute and analyse the reachability graph or basis reachability graph of the original Petri net, which in practice reduces the computational overheads as exposed by experimental studies. Examples are presented to demonstrate the proposed method.
- **Adaptive Supervisory Control of Automated Manufacturing Systems With Unreliable Resources Based on Smart Switch Controllers**
  Authors: Ziliang Zhang ; Gaiyun Liu ; Zhiwu Li
  Abstract: This paper proposes an adaptive supervisory control policy for an automated manufacturing system (AMS) with multiple types of unreliable resources. The considered AMS is a generalized system of simple sequential process with resources (GS3PR). In order to model resource failures and recoveries, modified recovery subnets are developed, which model more complex resource failure scenarios compared with traditional recovery subnets. For the purpose of guaranteeing the execution of a system's production successfully, from the perspective of the structural analysis of the system, a siphon control-based technique is introduced and a type of controller is developed. It is verified that the proposed adaptive control policy assures the deadlock-freeness of the controlled system no matter if there exist resource failures, and retains all behavior of the original system. Finally, examples are presented to demonstrate the proposed method.
- **Active Fault Diagnosis for Uncertain LPV Systems: A Zonotopic Set-Membership Approach**
  Authors: Zhao Zhang ; Xiao He ; Donghua Zhou
  Abstract: Active fault diagnosis (AFD) techniques can improve fault diagnosis performance by designing a set of appropriate auxiliary inputs and injecting them into the system to stimulate fault characteristics. The AFD problem for uncertain linear parameter-varying (LPV) systems with bounded external disturbances is studied based on a set-membership approach in this paper. Based on zonotopes, a set-membership observer is designed to estimate system states to reduce the influence of external disturbances, which aims to reduce conservatism. A F_W -radius-based criterion is minimized to get the optimal observer gain matrix. Because of the system uncertainties, the generator matrices of the output sets will have elements associated with the auxiliary input. A method is proposed to eliminate the relationship between the auxiliary input and the generator matrices, and a mixed-integer quadratic program (MIQP) is constructed to get the auxiliary input. By solving the optimization problem, the auxiliary input is designed for the considered finite kinds of faults to achieve fault diagnosis. Finally, numerical simulations are presented to demonstrate the effectiveness of the proposed approach.

Back to the contents

1.6. IEEE Transactions on Cybernetics

Volume: 54, Issue: 11, November 2024

- **Distributed Pinning Control: Stabilizing Large Boolean Networks Subjected to Perturbations**
  Authors: Qinyao Pan ; Jie Zhong ; Tatsuya Akutsu ; Yang Liu ; Rongjian Liu
  Abstract: Stability maintenance in systems refers to the capacity to preserve inherent stability characteristics. In this article, stability maintenance of large boolean networks (BNs) subjected

to perturbations is investigated using a distributed pinning control (PC) strategy. The concept of edge removal as a form of perturbation is introduced, and several criteria for achieving global stability are established. Two forms of distributed PCs, one implemented before perturbation occurs and the other after, are introduced. It is noteworthy that the designs of the controllers are solely dependent on the system's in-neighbors. The proposed method significantly decreases the computational complexity, reducing it from $O(2^{2|V|})$ to $O(|V| + |E| + \kappa \cdot 2^K)$, where $|V|, |E|$ denotes the cardinality of vertices and arcs of the adjacent graph of BN, κ is the number of the pinning nodes, and K represents the maximum in-degree of the network. In the worst-case scenario, the computational complexity is bounded by $O(|V| + |E| + \kappa \cdot 2^K)$. To validate the effectiveness of the proposed methods, results from multiple gene networks are presented, including a model representing the human rheumatoid arthritis synovial fibroblast, among which only 12 of the 359 nodes are deemed essential.

Back to the contents

1.7. IEEE/CAA Journal of Automatica Sinica

Volume: 11, Issue: 11, November 2024

- **Probabilistic Automata-Based Method for Enhancing Performance of Deep Reinforcement Learning Systems**

  Authors: Min Yang ; Guanjun Liu ; Ziyuan Zhou ; Jiacun Wang

  Abstract: Deep reinforcement learning (DRL) has demonstrated significant potential in industrial manufacturing domains such as workshop scheduling and energy system management. However, due to the model's inherent uncertainty, rigorous validation is requisite for its application in real-world tasks. Specific tests may reveal inadequacies in the performance of pre-trained DRL models, while the "black-box" nature of DRL poses a challenge for testing model behavior. We propose a novel performance improvement framework based on probabilistic automata, which aims to proactively identify and correct critical vulnerabilities of DRL systems, so that the performance of DRL models in real tasks can be improved with minimal model modifications. First, a probabilistic automaton is constructed from the historical trajectory of the DRL system by abstracting the state to generate probabilistic decision-making units (PDMUs), and a reverse breadth-first search (BFS) method is used to identify the key PDMU-action pairs that have the greatest impact on adverse outcomes. This process relies only on the state-action sequence and final result of each trajectory. Then, under the key PDMU, we search for the new action that has the greatest impact on favorable results. Finally, the key PDMU, undesirable action and new action are encapsulated as monitors to guide the DRL system to obtain more favorable results through real-time monitoring and correction mechanisms. Evaluations in two standard reinforcement learning environments and three actual job scheduling scenarios confirmed the effectiveness of the method, providing certain guarantees for the deployment of DRL models in real-world applications.

Back to the contents

2 Conferences

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

2.1 **2024 IEEE Conference on Decision and Control (CDC)**
Milan, Italy, December 16-19, 2024.
https://cdc2024.ieeecss.org/

2.2 **2025 ACM International Conference on Hybrid Systems: Computation and Control (HSCC)**
Irvine, California, USA, May 6-9, 2025.
https://hscc.acm.org/2025/

2.3 **2025 IEEE International Conference on Robotics and Automation (ICRA)**
Atlanta, USA, May 19-23, 2025.
https://2025.ieee-icra.org/

2.4 **2025 Annual Learning for Dynamics & Control Conference (L4DC)**
Ann Arbor, Michigan, USA, June 4-6, 2025.
https://sites.google.com/umich.edu/l4dc2025/

2.5 **2025 IFAC Workshop on Smart Energy Systems for Efficient and Sustainable Smart Grids and Smart Cities (SENSYS 2025)**
Bari, Italy, June 18-20, 2025.
https://conferences.ifac-control.org/sensys2025/

2.6 **2025 European Control Conference (ECC)**
Thessaloniki, Greece, June 24-27, 2025.
https://ecc25.euca-ecc.org/

2.7 **2025 American Control Conference (ACC)**
Denver, Colorado, USA, July 8-10, 2025.
https://acc2025.a2c2.org/

2.8 **2025 International Conference on Automation Science and Engineering (CASE)**
Los Angeles, California, USA, August 17-21, 2025.
https://2025.ieeecase.org/

2.9 **2025 IEEE Conference on Control Technology and Applications (CCTA)**
San Diego, California, USA, August 25-27, 2025.
https://ccta2025.ieeecss.org/

2.10 **2025 IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)**
Porto, Portugal, September 9-12, 2025.
https://etfa2025.ieee-ies.org/

2.11 **2025 International Conference on Systems, Man, and Cybernetics (SMC)**
Vienna, Austria, October 5-8, 2025.
https://www.ieeesmc2025.org/

Back to the contents

3 Books

3.1 Cybersecurity of Discrete Event Systems—From Smart Attacks to Resilient Defence

Author: Rong Su, Nanyang Technological University.

Description: This book describes analysis and control against smart cyberattacks in discrete event systems (DES), modelled by regular languages or finite-state automata. “Smart attacks" cannot be detected by the supervisor until an irreversible process towards ensured damage occurs. An attack may be conducted either in the observation channel (i.e., the input of the supervisor) or in the command channel (i.e., the output of the supervisor), or both simultaneously. Therefore, defense strategies against these attacks are urgently needed. This book provides an overview of the latest theories and includes empirical examples to illustrate concepts and methods. By centering on what information is available and how such information is used, the readers are provided with methods to evaluate the cyber vulnerability of a given system and to design a resilient supervisor against relevant smart attacks. By focusing on a conceptual introduction and systematic analysis, this book provides a solid theoretical foundation for future exploration by researchers and graduate students who are interested in cybersecurity research, not necessarily limited to those in the DES community. Readers are recommended to have a background in formal language theory.

Additional information on the book can be found at
https://www.routledge.com/Cybersecurity-of-Discrete-Event-Systems-From-Smart-Attacks-to-Resilient
Su/p/book/9781032368108?srsltid=AfmBOor9fqjhOR7YfMgGE8coz0rHXF6YyKhoucc7UzqYlY9GhcWpQBg3,
where an inspection copy is possible for educational institutions.

3.2 Graph-Theoretical Methods in Systems Theory and Control

Author: Jan Lunze, Ruhr-University, Germany

Description: The book describes for numerous scenarios how to use the structural properties of a system represented by a graph to simplify modelling, analysis, and design tasks. For example, block diagrams and coupling graphs can be used to decompose systems, automata graphs to analyse discrete-event systems and Markov chains, structure graphs to find generic properties of linear systems or communication graphs to design networked control systems. The book includes many examples derived from diverse fields of application, exercises with solutions and MATLAB scripts to implement graph-theoretical methods for systems analysis.

Additional information on the book can be found at
www.editionmora.de/gmsc

The book is produced as “print-on-demand" and can be ordered directly at the printer:
https://publish.bookmundo.de/books/349971

3.3 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).

Back to the contents

4 Software Tools

4.1 Eclipse ESCET™ version 5.0 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 toolkit's website at https://www.eclipse.dev/escet/.

In October 2024, ESCET version 5.0 has been released and can be downloaded from https://www.eclipse.dev/escet/download.html. he main changes in this version are

- Annotations are now a stable CIF language feature.
- The CIF data-based synthesis tool now has a new 'Exploration strategy' option, featuring not only regular fixed edge order and the workset algorithm, but also a new third strategy: the saturation strategy. This new saturation strategy improves the performance of reachability computations. On average, for the CIF benchmark models, synthesis performance is improved 14.5 times, although the results differ per model. Saturation is now the new default exploration strategy. The 'Edge workset algorithm' option is no longer supported.
- The CIF controller properties checker now computes bounded response differently, using the execution scheme, which improves the performance of the check, and generally leads to lower bounds. Furthermore, the CIF controller properties checker now uses the saturation strategy for reachability computations, improving the performance of the non-blocking under control check.
- Several improvements to the (still experimental) new CIF PLC code generator have been included. The CIF code generator now generates code that adheres to the execution scheme prescribed by the CIF controller properties checker (see point above). As a result of this, some parts of the generated code are now in a different order.
- The CIF to mCRL2 transformer has been re-implemented and is now based on first linearizing the CIF specification. For recursive process call, now only the assigned variables are included, not all variables, and the arguments are named rather than positional, which reduces the model size and improves readability. No more summations, nor location pointers (sorts) for automata with only one location, are generated. See release notes for detailed changes in the CIF to mCRL2 transformer.

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.dev/escet/release-notes.html.

Back to the contents