OUKA
The University of Osaka
Institutional Knowledge Archive

Title	Abstraction-based Formal Synthesis for Cyber-Physical Systems Using Approximate Alternating Simulation
Author(s)	溝口, 将史
Citation	大阪大学, 2023, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/92194
rights	
Note	やむを得ない事由があると学位審査研究科が承認したため、全文に代えてその内容の要約を公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

様式３

論　文　内　容　の　要　旨

氏　名　（　溝　口　将　史　）	
論文題名	Abstraction-based Formal Synthesis for Cyber-Physical Systems Using Approximate Alternating Simulation (近似交替模倣を用いたサイバーフィジカルシステム向け形式的抽象化コントローラ設計法)

論文内容の要旨

形式的制御系設計法は、制御対象の制御仕様の充足を設計時に理論的に保証する”correct-by-design”を実現する手段として注目を集めている。形式的制御系設計法をサイバー物理システムに適用するためには、制御対象を有限の状態数で抽象化すること(finite abstraction)が不可欠である。なぜなら制御対象はしばしば無限の状態数を持つ遷移システムとして記述され、有限時間内での解析が困難だからである。本論文では、部分可観測な制御対象、一定の入力むだ時間のある制御対象、およびネットワーク接続された制御対象に対して抽象化に基づく形式的制御系設計法を拡張した。部分可観測な制御対象に対し、観測出力に基づき制御対象がとりうる状態を推定するオブザーバを設計した。むだ時間が存在する制御対象に対し、古典制御のスミス法から着想を得たシンボリックスミス制御器を設計した。ネットワーク接続された制御対象に対し、観測出力と制御入力列とネットワークプロトコルとに基づき制御対象の状態を予測しネットワーク外乱の影響を抑制した。これらの適用結果に基づき、本論文では、「シンボリック制御バリア関数」なる概念を提案し、制御対象がセーフティプロパティを充足するよう制御系を設計する手法を開発した。抽象化モデルを用いてセーフティを実現するため、シンボリック制御バリア関数は保守的に構築される。すなわち、抽象化モデルの中で同じ状態に抽象化されうるあらゆる制御対象の状態のうち、セーフティプロパティに対して最も厳しい状態においてもセーフティプロパティが満たされるようにする。結果として、抽象化モデルに対してセーフティプロパティを満たす制御器が存在すれば、その制御器を制御対象向けに詳細化(refinement)することにより、制御対象がセーフティプロパティを充足することが証明される。これが本論文の主要成果である。さらに、観測データからシークレット情報を特定できないオパシティと呼ばれる性質をセーフティハイパープロパティに変換することで、オパシティを満たす制御系設計手法を開発した。

様式７

論文審査の結果の要旨及び担当者

氏　名　（　溝　口　将　史　）		
	（職）	氏　名
論文審査担当者	主査　教授	潮　俊光
	副査　教授	乾口雅弘
	副査　教授	飯國洋二

論文審査の結果の要旨

本論文は、制御対象の状態を所定の領域から逸脱させない安全制御を考え、その実現方法として制御バリア関数を用いた手法を提案している。さらに、オパシティを充足する制御系設計を行っている。第１章の緒論と第６章の結論を含め、以下の各章から構成されている。

第２章では、形式的制御系設計手法の概略をまとめている。特に、状態数が無限で非決定遷移を有する制御対象を有限の状態数で近似して制御系設計を行う旨が述べられている。

第３章では、従来は完全可観測かつむだ時間のない制御対象にのみ適用可能であった形式的制御系設計手法を、部分可観測な制御対象やむだ時間を有する制御対象に対して適用可能とするよう拡張している。制御対象のとりうる状態を複数予測し、どの予測に対しても共通して制御仕様を満たす制御入力を選択する手法が記されている。

第４章では、制御バリア関数を形式的制御系設計手法に導入している。特に非決定遷移に着目し、安全領域に対して最も厳しい状態に遷移した場合であっても安全領域から逸脱しないよう考慮されている。タンク水量を一定範囲に保つ制御を例題に、手法の妥当性が示されている。

第５章では、システムの初期値がシークレット領域に含まれていたか否かを外部から隠匿する初期値オパシティ制御問題が考察されている。シークレット領域内の初期値から始まる振る舞いと領域外から始まる振る舞いを同時に考え、それらが互いに類似した観測列を出力し続けることを要請し、これを安全制御問題に帰着させている。タンク水量制御を例題に取り上げて、初期値オパシティを満たす制御系を設計している。

以上のように本論文は、形式的制御系設計手法の適用対象を拡張するとともに、安全制御を可能とし、さらにその応用としてオパシティを充足する制御系を構築し、形式的制御系設計手法の発展に貢献した。よって、博士（工学）の学位論文として価値のあるものと認める。