

超高信頼ソフトウェアシステム検証学研究室

(国立研究開発法人宇宙航空研究開発機構)

http://stage.tksc.jaxa.jp/jedi/JAXALab/index.html http://stage.tksc.jaxa.jp/jedi/index.html



(写真左から)

客員教授：片平 真史 masa-katahira@is.naist.jp

客員教授：石濱 直樹 ishihama@is.naist.jp

宇宙開発の実データに触れ、あなたの研究成果で新たな宇宙を創り出そう

研究を始めるのに必要な知識・能力

まずは、超高信頼性が求められる宇宙や自動車分野に興味があること。実際の宇宙分野のソフトウェア開発に関するデータを用いて、新たな方法論を創造する研究となるため、ソフトウェア工学、統計学の基礎知識が必要。

研究室の指導方針

学生自身で課題を抽出し、解決するための方法を創造するプロセスを体験することで、主体的に考える人材を育成します。修士1年では、課題意識、興味のあるテーマを自身で探索できるようにアドバイスをしながら研究テーマを絞り込みます。研究テーマに合った宇宙分野の実データを提供し課題抽出のための分析を行います。修士2年では、データに基づく方法論を考案し、実証実験を行います。また、研究テーマにより、NASAや欧州宇宙機関(ESA)との共同研究に参加してもらいます。

この研究で身につく能力

研究テーマに依らず、自身で考え、解決できる思考能力が身につく。また、失敗が許されない社会インフラシステムに必要な高信頼性、安全性確保のために、重要となる不具合・失敗要因の基礎知識を習得でき、解決策となるソフトウェア開発技術、ソフトウェア検証技術を宇宙分野での実証経験(ノウハウ、留意点)を含めて習得でき、今後の応用力をつけることができる。

修了生の活躍の場

宇宙関連企業、PwCあらた監査法人、村田機械、富士通

研究内容

今日、組み込みシステムや社会インフラシステムは、国家や人命の安全を支える根幹として位置づけられており、それらの超高信頼性を確保することは社会全体の安全性を高める上での最重要課題の一つです。超高信頼ソフトウェアシステム検証学研究室では、宇宙航空研究開発機構 研究開発部門 第三研究ユニットの持つ、宇宙システムにおける超高信頼性や安全性に関する研究および実践における高い実績にもとづいて、極限環境で正しい動作が求められるソフトウェアの超高信頼性・安全性を実現するためのソフトウェア検証方法論を研究します。特に、現在の重要課題である、人工知能などによる不確実性のある複雑なソフトウェアシステムの検証網羅性保証に必要な以下の方法論を研究・教育します。これらの研究成果は、宇宙システムに限らない、社会基盤システム全般の超高信頼化への応用が期待されています。

1) 高信頼性・安全性検証手法

ロバスト性検証技術

仕様外要求を含めたロバスト性検証の要素技術、検証環境の自動生成アルゴリズムや方法論を研究・開発します。

検証自動化技術

システム構成、運用条件、不具合パターンモデルなどを用いた検証ケース自動生成及び自動合否判定のためのアルゴリズムや方法論を研究・開発します。

2) 高信頼性・安全性評価手法

安全性評価手法

システム安全分析手法(STAMP/STPA, FRAM)を用いた、人工知能などによる不確実性のある検証が困難なソフトウェアシステムに対する検証手法の検討。または一般的な安全要求に基づく安全性評価手法の確立。

モデルベースミッション成立性評価手法

SysmlやUML等のモデルを用いたシステム設計をする際に、開発の早い段階からミッション成立性を評価する手法を研究します。

検証網羅性評価技術

複数のソフトウェアシステムから構成される多種の検証情報に基づきソフトウェアシステム全体の検証網羅性を評価する技術(アシュアランスケースなど)を研究します。

欠陥伝搬評価技術

ソフトウェアシステム全体の欠陥モードの体系化及びそのシステムへの影響度評価手法を研究・実証します。



図1 「ロバスト性検証技術・自動検証技術の概念図」



図2 「アシュアランスケースを用いた検証網羅性評価」

研究業績・共同研究・社会活動・外部資金など

論文誌

・柿本和希, 川口真司, 高井利憲, 石濱直樹, 飯田元, 片平真史, "Goal Structuring Notationを用いた汎用的な安全要求の明確化と評価," SEC journal, number 47, pages 16-23 2016年12月

国際会議(査読付き)

・Mitsuaki Tsuji; Toshinori Takai; Kazuki Kakimoto; Naoki Ishihama; Masafumi Katahira; Hajimu Iida, Prioritizing Scenarios based on STAMP/STPA Using Statistical Model Checking, 2020 ICSTW

国内会議(査読付き)

・柿本和希, 川口真司, 高井利憲, 石濱直樹, 飯田元, 片平真史, "CBCS 安全要求の適用性向上に向けた可視化の取り組み," クリティカルソフトウェアワークショップ, 2016年

受賞

[1]柿本和希, 川口真司, 高井利憲, 石濱直樹, 飯田元, 片平真史, "「SEC journal」論文賞 所長賞," SEC journal, 2016年11月.

[2]柿本和希, 川口真司, 高井利憲, 石濱直樹, 飯田元, 片平真史, "第13回クリティカルソフトウェアワークショップ 最優秀賞," 第13回クリティカルソフトウェアワークショップ, 2016年.