GrammaTech,火星探査機キュリオシティが成し遂げた生命体調査を支援

8ヶ月、3億5千200万マイルに及ぶ飛行の後、NASAの火星探査機キュリオシティは、巨大なパラシュートとジェット制御により降下し、スカイクレーンと呼ばれるバンジーのような機器の支援により、見事に着陸に成功しました。火星と地球間では通信時間を要するため、着陸手順は完全にソフトウェアにより制御されました。そのソフトウェアの信頼性を高めるために、NASAは先進的な静的解析を使用しました。

キュリオシティの着陸は、完全にソフトウェアにより制御されました。そのソフトウェアの信頼性を高めるために、NASAは先進的な静的開発ツールを使用しました。

最も先進的な技術により作成されたキュリオシティは、小さなSUVの移動実験室のような物です。搭載される17個のカメラ、ロボットアーム、実験室用の特殊な機器等は、2百万行以上のソフトウェアにより制御されます。

不具合ゼロのソフトウェア開発

宇宙船のミッションを成功させるためには、ソフトウェアが大きなカギを握っています。キュリオシティは、以前の火星探査機よりもソフトウェアに大きく依存しています。障害保護システムでさえも、ソフトウェアがベースになっています。

発射の2年前から、NASAは、ミッションクリティカルで、不具合ゼロのソフトウェア開発に焦点を置いてきました。全てのコードは、GrammaTech社のCodeSonar®を含む先進的な静的解析ツールにより解析が行われました。NASAに協力したGrammaTechのシニアサイエンティスト、Michael McDougallは、「NASAのジェット推進ラボは、キュリオシティのソフトウェアのバグをチェックするために、毎夜、CodeSonarを使用しました」と述べています。

先進的な静的解析では、バッファオーバーラン、競合状態（レースコンディション）、ヌルポインタ参照、リソースリーク等の重大なソフトウェアの不具合を見つけることができます。また、冗長な条件、無意味な割り当て、未到達コード等の不具合も検出可能です。GrammaTechの技術副社長のPaul Andersonは、「静的解析は、コンパイル時に行われるので、ソフトウェア開発中に不具合を見つけることが可能です。ツールは、パスや条件、プログラムの状態を抽象的に解析するので、通常のテストでは実現することが不可能な非常に高いテスト網羅度を達成することが可能です」と述べています。

キュリオシティのソフトウェア・アップグレード

火星への着陸時に、キュリオシティは、4日分の着陸用ソフトウェアの消去と地表オペレーション用のプログラムのインストールに関するメジャーアップデートを行いました。
NASAは、異なったミッションで必要とされる各ソフトウェアがアップグレードできるように設

「NASAにとって、これは大きな技術的成果であり、この成功に我々が貢献できたことをうれしく思います」

– Michael McDougall,
GrammaTech
シニアサイエンティスト

計しました。ソフトウェアのアップグレードが必要になるのは、キュリオシティの計算能力が地上で使用される物に比べて低いためです。しかしながら、RAD750PowerPCマイクロプロセッサは、スマートフォンやラップトップでは不可能な高いエネルギーの宇宙線に耐えることができます。また、32ギガバイトのスマートフォンに比べ、4ギガバイトしかメモリ容量を搭載していません。

ミッションの各フェーズでの新たなソフトウェアは、その都度開発されました。なぜならば、一つの不具合が探査機との通信を失い、ミッションを危険にさらすことになってしまうからです。全てのソフトウェアのアップグレードは、最初に実行される時から完璧に動作する必要があります。

ミッションクリティカルなソフトウェア向けコーディング規約

NASAは、高品質ソフトウェア作成の為の優れた記録追跡手法と共に、いくつかのベストプラクティスに沿った開発をしています。厳密な開発プロセスの一部として、火星探索キュリオシティのミッションでは、NASAのJPL信頼性ソフトウェアラボ(LaRS)で開発された「Power of 10：セーフティクリティカル向けコード開発ルール」を遵守しています。GrammaTechは、NASAと共同で、静的開発ツールCodeSonarに、「Power10コーディングルールチェック」を追加しました。

JPLは、コーディングルールの開発の為に、過去数十年に渡るミッションにおいて発見された不具合を検討し、それらのミッションで共通に出現する不具合のリストを作成しました。そこから、非常に少ないが、明らかにリスクに繋がる、容易に覚えることができるルールを定義し、それが守られているかどうかを自動的に検証できるようにしました。10のルールは、ミッションクリティカルなソフトウェアのリスクを軽減するように設計され、飛行ソフトウェアの開発の標準コーディングとしてJPL内で展開されました。10のルールは、先進的な静的開発ツールに定義されており、開発プロセス中で積極的に使われるべきです。

「GrammaTechが、キュリオシティの着陸成功に関与できたことを大変誇りに思います。NASAにとって、これは大きな技術的成果であり、この成功に我々が貢献できたことをうれしく思います」と、McDougallは述べています。

キュリオシティは継続して新たな発見をしています。毎日100名のエンジニアと研究者が探索機に命令を送り、生産的に科学的な成果を集めています。必要に応じたソフトウェアのアップグレードにより、NASAは火星に関する新たな疑問に答えています。

株式会社エーアイコーポレーション

日本代理店
株式会社エーアイコーポレーション
www.aicp.co.jp

GRAMMATECH

GrammaTech, Inc.
531 Esty St.
Ithaca, NY 14850 USA
電話：607.273.7340
www.grammatech.com

写真提供NASA