

(株)不二越 ロボット事業部様の IEC61508機能安全認証への取り組みと 単体テストツール「カバレッジマスターwinAMS」の適用事例

近年、各業界において、機能安全認証に対する取り組みが盛んになっています。「機能安全規格」とは、安全な製品を開発するために有効と考えられる管理や手法への適用を定めたもので、安全に関係する事項を規格化し、安全な製品の開発のために作られたものです。機能安全規格は国際規格である「IEC61508」をベースとして、自動車向けISO26262を始め、各製品カテゴリごとに策定されています。

ガイオでは、機能安全認証のための組込みソフトウェアテストツールを提供していますが、今回、産業用ロボットの開発を手がける(株)不二越 ロボット事業部様に、機能安全認証IEC61508への、ガイオの単体テストツール「カバレッジマスターwinAMS」の適用事例についてインタビューをさせていただきました。

【インタビューさせて頂いたお客様】

(株)不二越 ロボット事業部 浜畑 光晴様 杉岡 和実様



IEC61508の認証に向けての取り組みのスタート

(株)不二越 ロボット事業部様は、2004年頃から産業用ロボットの機能安全認証に対する取り組みを開始し、既にあったISO9001品質マニュアルをベースに、機能安全認証の要求に合わせたプロセスやドキュメントを整備する活動からスタートしました。この経緯について伺いました。

4年ほど前になりますが、最初に弊社の単体テストツールをご検討頂いた当時、先にIEC61508認証について活動を進められていたと伺っていますが、その当時の状況はいかがだったのでしょうか？

不二越 浜畑様：

最初は、IEC61508の認証を行っている外部の企業から情報を得る所から始めました。例えば、カバレッジ計測やその他テストツールにどのようなものを使っているかを聞き出して、そこから、カバレッジマスターやその他の静的解析ツールのことを知りました。

それは、御社と同じような産業用ロボットを開発されている会社からですか？

不二越 浜畑様：

いいえ、安全機器を開発している他業種のメーカー様からでした。当時、弊社はまだツールに関する情報をあまり持っていませんでしたが、あるメーカーの方から「こんなツールがあるよ」という紹介を受けたと記憶しています。ちょうど展示会(組込みシステム開発技術展)がありましたので、ガイオさんのブースで現物を見て、使って見ようかという事になったと思います。

弊社のツール以外では、IEC61508の認証に向けてどのような取り組みをされたのでしょうか？

不二越 浜畑様：

まず、当時は、何から手を付けたら良いのかがさっぱり分からない状態でしたので、どのようにすれば良いかについて、自分自身が考えた方法で合っているかを、認証機関に相談し確認することから始めました。例えば、ISO9001の品質マニュアルや標準ドキュメント等が既にあったのですが、これをベースに機能安全に適するドキュメントを整備するためには、認証機関との間で、どのようなやりとりが必要か、どのような手順が必要かとかを、IEC61508の原文を読んだ上で相談に行きました。このようにして、不二越独自のマニュアルに上げてゆく事からスタートしました。

そのような認証機関とのやりとりなど、専任の方がかかりっきりで行うような状態だったのですか？

不二越 浜畑様：

最初は、品質マニュアルに近い所を扱っていたので、マネージャーが中心となって、マニュアルを仕上げてゆく活動を行っていました。ISO9001の品質システム全体と、機能安全の内容とどこが違うのか、どこを直さなければならぬのかを開発関係者全員で仕上げました。

マニュアルを直すために、どう取りかかって行くかを計画しながら、それと並行して、安全機器を作っているメーカーさんから情報を得る活動をしていました。当時は、海外では安全ネットワークと言うのが流行りだしていましたので、国内でもその動きがあり、情報をやりとりする場となっていました。

安全に関するワーキンググループにも加わり、情報収集をしました。メーカーによって安全システムは別々の物ですので、その中身まで聞くことはできないのですが、何をプラスして行けば良いかとか、全く知らない内容に付いては素直にどうすればよいのかを技術者レベルで意見交換していました。

このお話は、今から5年ほど前だと思いますが、取り組み自体が2005年頃から始まったと言うことでしょうか？

不二越 浜畑様：

丸々2年くらいはこの活動をやったと思います。カバレッジマスターを購入した時より1年以上前からスタートしていますので、やり始めたのは2004年から2005年にかけてでした。このときは、まだ国内の安全性に関するワーキンググループで認証の話は出ておらず、ヨーロッパのワーキング活動が有名だったので、そこにも聞きに行ったりしていました。これがスタートした当時の状況です。

IEC61508のAppendixの中には、このような技法を使いなさいとか、ツールを使いなさいとかあったと思いますが、不二越様のなかで取り組んだことは何かありますか？

不二越 浜畑様：

全て初めてだったので、認証機関の方には「どうすればよいでしょうか？」ではなく、「このような方法でやろうと思っているがどうでしょうか？」と言う聞き方で情報を聞き出していました。SIL安全レベルの規定には行わなければならないことが多く書かれているのですが、全てやった訳ではなく、安全レベルを満たす項目を選択して、選択した内容がそれでよいかを確認したと言う感じでした。

機能安全認証に向けてのソフトウェアテストについて

(株)不二越 ロボット事業部様には、ソフトウェアの単体テストツールとして、ガイオの「カバレッジマスターwinAMS」を採用頂いています。このツールを検討したきっかけや採用のポイントについて伺いました。

ソフトウェアのテストと言う部分では、どのように進めて行ったのでしょうか？

不二越 浜畑様：

テストについて検討したのは、活動のかなり後の方でした。カバレッジマスターを購入した2006年頃は、既に機能安全の導入プロジェクトでソフトウェアのかかなりの部分は作っていました。ソフトウェアテストについて考えたのは、仕様書を書く段階あたりでした。規格の中には、最初に機能安全要求仕様書がありますが、そこにはどのようにして安全を実現するかを書かなければならないのです。この中で、例えばどのようにメモリチェックを行って、どのように安全を実現するかを書く必要があり、その後、テスト計画を作る際に、単体テストツールとして採用したカバレッジマスターや、静的解析ツールの名前などを書いて行きました。



カバレッジマスターwinAMSはどのような所が、御社のテストにインパクトがあったのでしょうか？

不二越 杉岡様：

ソースコードをできるだけ書き換えずにテストが行える所だと思います。関数の単体テストを行う際には、これまでは関数を抜き出して、関数をコールする別のプロジェクトを作って、引数にデータを与える様なコードを書いて、単体テストを行っていました。ここに大きな手間がかかっていたのですが、カバレッジマスターだとほとんど手間がかからなかった所が大きいと思います。このツールにより単体テストを行う範囲で、認証会社からもOKという評価を得ることができました。

認証という観点では、弊社のカバレッジマスターは御社にどのように役に立っているのかをお聞かせ頂けませんか？使ってみて、何か現場の意識に変化が起きたなどでも結構ですが。

不二越 杉岡様：

組込みシステムで実オブジェクトを使ってカバレッジが計測できるというツールは、今までに無かったと思います。パソコンでデバッグや確認をする分には十分やれていましたが、これはあくまでパソコンレベルであって、マイコンレベルにまでは手が届いてなかったと思います。これが実現できるツールであった事が、大きなポイントだったと思います。



従来は、カバレッジを計測することにあまり意識が向いていなかったかも知れませんが、カバレッジマスターを使うことで、C0は100%、C1は可能な限りと言う様な網羅性を確保しようと言う意識ができたと思います。

機能安全認証を通じて得たソフトウェア品質改善効果

カバレッジマスターwinAMSを使用した単体テストは、認証に対する成果はもちろんのこと、開発者の品質に対する意識改善にも効果がありました。どのように品質改善に結びついたのかを伺いました。

認証をきっかけにカバレッジマスターを適用することで、コードを網羅テストすると言うことでは、効果があったと言うことですね。

不二越 杉岡様：

そうですね。その他では、結果が残ることや、テストレポートを定式化できることも、カバレッジマスターの適用効果としては大きいと思います。

認証に必要な単体テストのエビデンスは、どのようにして作成したのですか？

不二越 杉岡様：

カバレッジマスターから出力されるカバレッジ計測結果や入出力テスト結果のCSVファイルをそのまま添付する形で対応できました。ですから、特に大きく手を加える様な手作業は必要ありませんでした。

全ての関数に対して、テストを行いレポートを作成したと言うことですか？

不二越 杉岡様：

そうです。全ての関数のレポートを作りました。結構な紙の束になりました。この時の認証対象は、安全機能の部分だけでしたので、規模としては、200～300関数でした。認証機関から、レポートのフォーマットに関しての指摘などは無かったですね。決められたテストがきちんと行われていることの確認が中心でした。

IEC61508の認証をきっかけに単体テストを行ってみて、何が効果的だったのでしょうか？

不二越 杉岡様：

単体テストの取り組みは、やはり結果が定量的に出たことが、ソフトの品質を考える上では良かったと思います。数字が出ることで達成感もありました。テストの工程で見つかった不具合もいくつかありました。

テストケースを考えることが、パスや分岐を見ながらソースコードをもう一度チェックする良い機会になったことは確かです。テストケースを作りながらソースを眺めている間にバグを見つけることができましたので、カバレッジマスターの適用をきっかけに、単体テストに取り組んだことは、認証目的以外にもプラスに傾いていると思います。

設計者の品質意識が変化したと言うことはありませんか？

不二越 浜畑様：

確かに、設計者の品質意識は上がりました。IEC61508の規格を読むことで、ソフトウェアだけでなくハードウェアについても多くのことが書かれていて、この内容を認証に必要な事と捉えるだけでなく、開発をチェックする手法として、今後も活かして行こうと考えるようになったと思います。

例えば、FMEAの場合であれば(FMEA= Failure Mode and Effect Analysis、故障モード影響解析)、信頼性だけでなく安全性を考える部分でのプラスアルファがあり、品質に良い方向に働いていると思います。ソフトだけでなくハードウェアの部分にも同様のことがあります。



ハード、ソフト両面での安全性に対する取り組み

今回の機能安全認証を適用した製品は、有人ラインでの産業用ロボットの安全性を確保するためのユニットに対してでした。安全性の設計とはどのようなものか、また産業環境におけるロボットの安全要求事項であるISO10218との関わりについても伺いました。

今回の認証ではソフトとハードではどのくらいの工数配分だったのですか？

不二越 浜畑様：

認証のための安全の設計は、ソフトとハードを合わせてどうするかで決まるもののなんです。工数ではソフトウェアの設計が8割くらいで、非常に膨大です。テストの工程は、ソフトとハードで半々位でしょうか？IEC61508では、故障モードでどうなるかのテストがあり、ハードのテストでは、部品が壊れたことを想定して、一点一点部品を外す、壊すと言うのを地道に行うのがあって、ソフトウェアで言えば、カバレッジを一行一行通して行くのと似ているのではないかと思います。

認証のための安全の設計は、9割アイデアなんです。と言うのは、どうやって安全を立証するかという最初の考え方だけでほとんどが決まってしまうということなんです。それが決まってくれば、後はソフトであれば、カバレッジマスターなどツールを使って、テスト項目を淡々とテストして行く感じです。

産業用ロボットの場合、ハード、ソフトに各々安全に関する機能が組み込まれると思いますが、今回の安全認証の対象になったのは、どのようなユニットなのですか？

不二越 浜畑様：

機械の部分は本来は頑丈であればよいということが基本であり、色々な動作範囲を取りますので、これをエレキの部分やソフトにより安全性を確保するかありません。今回のIEC61508認証を受けることになった機能ユニットは、ソフトウェアでこの動作範囲を守る部分です。

御社のロボットは、無人ではなく有人の製造ラインでも使われているのですよね？有人ラインに関するロボットの認証には、他の規格もあつたと思いますが？

不二越 浜畑様：

そうなんです。この分野にはISO10218(産業環境におけるロボットの安全要求事項)があります。今回はIEC61508から始まったのですが、これはそのままISO10218に展開していて、有人ラインで、人とロボットが共存している所で、人とロボットの境目をゼロにしようと言う考え方が求められます。



今回の認証対象の製品は、安全性を二重に付加するためのものです。通常のロボットにも当然安全性設計は入っていて、位置、速度、トルクを別に監視して、有人ラインでの安全性を二重にチェックするような部分になります。ロボットには、各動作部分に異常検知装置が付いており、通常はその異常検知が働くため、安全にできていたのですが、今回のものは、さらにこれを監視して安全性を確保するユニットです。

最後に、カバレッジマスターに話を戻しますと、何か使う上で不満があつたと言うことはありませんか？

不二越 浜畑様：

テストケースが膨大になると、実行時間が長いのが強いて言えば不満かも知れませんが。カバレッジマスターは元々、ツールとしてしか見ていなかったのですが、機能面がどうこう言うことは考えませんでした。ですが、結果的には、今回の認証のためのツールとして、ピッタリはまったと言う感じです。

これから機能安全認証を受けようとしている企業の方々に、非常に貴重なお話を頂けたと思います。ご協力を頂きまして、大変ありがとうございました。

(終)

まとめ

今回、不二越様へのインタビューでは、高い信頼性と安全性を両立させるための様々な取組みや工夫についてお話を伺うことができました。その中で機能安全規格への対応において、確実な単体テストを実現するという不二越様のニーズに、カバレッジマスターが応えることができたとのコメントをいただきました。

今後ともガイオ・テクノロジーは、お客様による機能安全規格へのご対応を確実にご支援できる様、最適なツールとソリューションを展開して参ります。
(ガイオ・テクノロジー営業部)

ユーザー情報

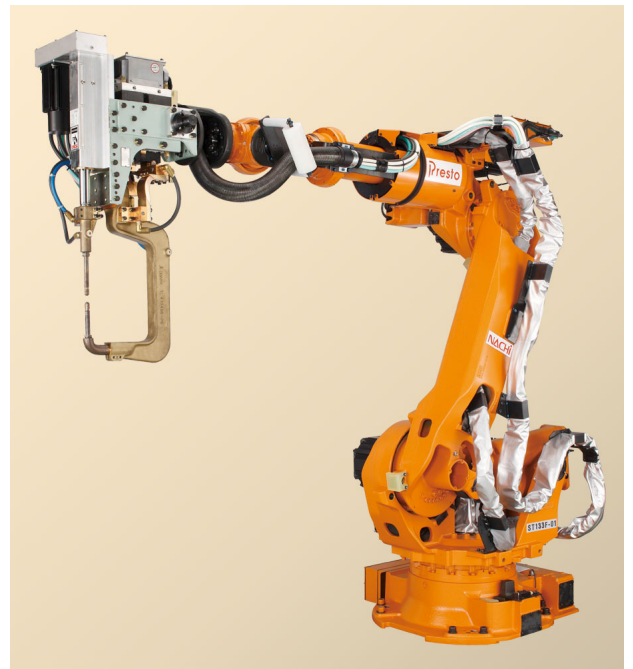
株式会社不二越 ロボット事業部 様

本社・富山事業所：

〒930-8511 富山市不二越本町1丁目1番1号 (TEL)076-423-5111

URL: <http://www.nachi-fujikoshi.co.jp/>

開発製品例：



カバレッジマスター winAMS

組込みマイコン完全対応！ C/C++ 組込みソフト向け モジュール単体テスト自動化ツール
フックコードを使わず 実装マイコンコードをそのまま動作させて単体テストを実行
静的解析ツール「CasePlayer2」と連携して C1、MC/DCの最適化テストケース作成をサポート
自動車分野の単体テストのデファクト、機能安全ISO26262認証に最適の検証ツール

組込みマイコン完全対応！ C/C++ 組込み向け モジュール単体テスト(ユニットテスト)ツール

システムテスト、結合テストだけでは発見できない「潜在化した不具合」を検出する方法として、組込み開発の広い分野で、単体テストが注目されています。また、自動車ソフト機能安全(ISO26262)の分野では、認証項目の1つに単体テストの実施が要求されています。

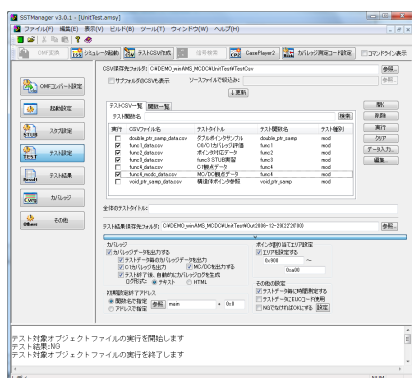
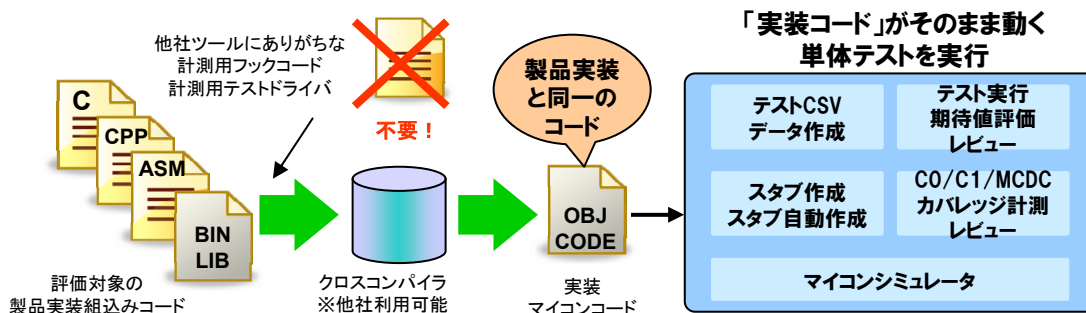
「カバレッジマスター winAMS」は、クロスコンパイラで生成した「実装マイコンコード」を評価対象として、マイコンシミュレータ(ISS)で単体テスト(ユニットテスト)実行を行う仕組みを持つテストツールです。Cソースの論理レベルでの単体テストに留まらず、組込み特有のマイコンへの実装に依存した問題点を含めた、信頼性の高いホワイトボックステスト、単体テストが行えます。

自動化されたC0、C1、MC/DCカバレッジ計測機能

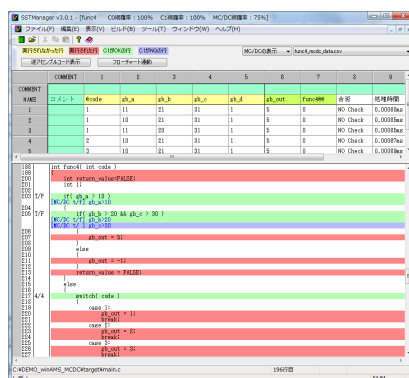
入出力テストを通じて、テスト網羅率を示すC0,C1,MC/DCカバレッジ結果を自動レポートします。テストデータとソース上の実行パスの対応を表示するビューを搭載しており、テスト結果の解析に利用できます。(※MC/DCカバレッジの計測機能は、オプションで提供されています。)

ソース解析に基づいた C1、MCDCカバレッジを満たす テストケース自動作成機能

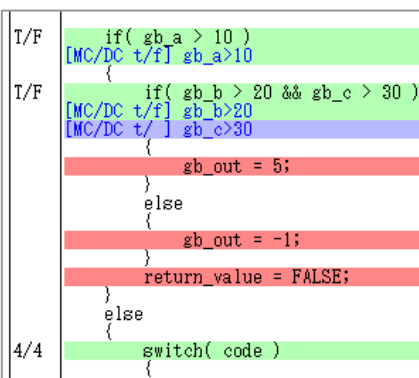
ソース解析ツール「CasePlayer2」との連携により、if、switch、for、whileなど、条件分岐着目したカバレッジ計測、C1/MCDCの要件を満たすためのデータを自動生成します。



SSTManager: カバレッジマスターwinAMSの単体テストプロジェクトの管理、テストデータ作成を行うアプリケーション



C0/C1/MCDCカバレッジビュー: テストデータとカバレッジ結果との解析が可能です



C1、MC/DCカバレッジ計測の例
(C1は網羅しているが、2つ目の複合条件式のうち、gb_c>30のFALSEの評価が未実行であることを示す)