
ツールの使用に対する安全性

今回のメールマガジンでは、ISO 26262 におけるツールの使用に対する安全性についてご紹介します。ISO 26262 対応においては、認定を受けたツールを使用しなければならないのでしょうかという質問をよくお聞きします。恐らくこの認識は、「Qualification of software tools」という ISO 26262 ドラフト段階で記述されていた、ツール認定(Qualification)に関する条項に基づくものと思われます。本条項の本質的な意図は、製品開発に使用する各種ツールが、想定した使用用途に対して安全上の問題を引き起こすリスクが十分に低く、問題なく受け入れることができるという安全性を裏付ける行為を要求しており、決して、認定を受けてさえいればそのツールをどのように使っても安全であることではありません。なお、正式発効された ISO 26262-8 では、「Confidence in the software tools」と記述され、ツールの使用に対する安全性を裏付けるための方法が記載されています。

それでは、ツールの使用に関する安全性はどうすれば正当に裏付けることができるのでしょうか。これまでツールの使用に関する正当性の証明を、ツールベンダーに一方的に求めているケースが見受けられますが、ツールベンダーにのみ求めるべきものでしょうか。仮に、ツールに不具合が存在しないことが証明されていたとしても、ツールを正しく使用していなければ、時として開発対象に不具合が混入してしまいます。
逆に、正しくツールを使用していたとしてもツール自身に不具合が存在していれば、ツールが誤った出力をしてしまい、この場合も開発対象に不具合が混入してしまいます。

ツールの使用に対する安全性を裏付けるためには、まずツールがどのような使用環境において、どのように使用するのかを分析する必要があり、その状況下で、ツールに不具合があった場合の影響度を特定します。これをシチュエーション分析と呼び、最終的に TI（Tool Impact、ツール影響度）として表現されます。
続いて、ツールの不具合の検出可能性を分析します。これは、同等の機能を持った異なるツールの計測結果が一致していることを確認するなどの方法で分析され、ツールの TD（Tool error Detection、ツールエラー検出度）として表現されます。TI と TD の関係から、TCL（Tool Confidence Level）という、安全性を裏付けるための対応の厳格さの目安が決まります。

[TCL の決定]

	TD1	TD2	TD3
TI1	TCL1	TCL1	TCL1
TI2	TCL1	TCL2	TCL3

TCL が決定した後の対応方法も、ツール開発のプロセス評価や、安全分析などいくつかの方法があります。例えば、「ソフトウェアツールの妥当性確認」（前提条件：TCL3、ASIL D）の場合、”使用要件とツールの適合性の実証”、”ツールの誤動作と誤出力時を含んだ分析”、”異常動作時のツールの反応の検討”が必要となります。

まず、ツールの仕様がツールの使用目的や環境条件などを満足していることを実証します。そのためには、ツールの要件を識別する必要があります。例えば、電圧計測の場合、実際に計測したい電圧範囲に対して、ツールの要件が計測可能な電圧範囲となっていること、または想定する使用環境においてツールが正常に動作可能であることということなどがこれに該当します。そして、それらの適合性を実証するためのテストケースを作成およびテストケースに基づいた検証を行い、ツールが期待する要件に適合していることを保証します。
次に、ツールの誤動作と誤出力時を含んだ分析が必要となります。ツールの誤動作と誤出力は、その影響や対処方法、検知方法を含め分析する必要があります。しかし、ツールの誤動作、誤出力などの発生条件や影響などは、使用環境によって変化するため、ツール使用者が全てを把握するのは困難です。その影響など知るためにはツール使用者がシチュエーション分析を行い、想定したユースケースにおけるツールの誤動作、誤出力の情報提供をツール開発者から受ける必要があります。そのほかに禁止された設定値の入力や動作可能温度を超えた状態でのツール使用における出力などといった異常条件下でのツール使用におけるツールの反応を検討する必要があります。しかし、これもツール使用者のみでは異常条件下の動作を知ることはできませんので、
ツール開発者の協力が必要になります。

このように、ツール使用の安全性を裏付けるためにはツール使用者、ツール開発者の協力が必要なのです。
(2012 年 02 月号 メルマガ抜粋)

ビジネスキューブ・アンド・パートナーズ株式会社
東京都渋谷区広尾 1-13-1 フジキカイ広尾ビル 5F
TEL：03-5791-2121 / FAX：03-5791-2122 / E-mail：consulting@biz3.co.jp
URL：http://biz3.co.jp