
ISO 26262 は私たちに何を求めているのか

今回は、ISO 26262 が私たちに求めていることについて考えてみたいと思います。今回は、ISO 26262 Part6 の中から、設計の表記法をテーマとして取り上げます。

安全なものづくりをするためには、安全に関する要件が確実に実装される仕組みが必要になります。ここでいう「確実に実装される」ということを実現するためには、「安全要件が正しく解釈されること」がまずは求められます。安全要件が適切に定義されていたとしても、それが正しく解釈されないことには、安全の実現はできません。これは、安全要件に限ったことではなく、安全に関連しない要件についても同様ですが、ISO 26262 では、「要件や設計内容が正しく解釈される仕組み」の導入が要求されています。
その要求事項とは、目標の ASIL や適用対象の特性に合わせて「自然言語」、「非形式的手法」、「準形式的手法」、「形式的手法」を適用することです。これらを適用する上で重要なことは、構文形式とセマンティック（意味表記）が表記法の適用目的や適用対象に対して適切な厳格さで適用されることです。
構文形式とは、文法、または図や表などの「表記ルール」を定めたものであり、セマンティックとは、記載される「意味の解釈の仕方」です。ISO 26262 では、仕様や設計の誤解釈を低減するために、これら構文形式とセマンティックの定義を求めています。

ここからは、「自然言語」で表記した例文を用いて、構文形式とセマンティックを説明し、「要件や設計内容が正しく解釈される仕組み」を考えていきます。以下の例文は、NPO 法人 組込みソフトウェア管理者・技術者育成研究会（SESSAME）の「話題沸騰ポット」の要求仕様書の内容を一部加筆したものです。

「水位センサが ON かつ満水センサが OFF の場合、温度制御が開始されます。水量に関するセンサと蓋センサが OFF の場合は、温度制御を停止します。」

まず、この文章の構文形式を見ると、「開始されます。」という表現がありますが、これは、受動的な現象なのか、能動的な現象なのか、曖昧さが存在します。また、この文章には、主語がなく、これも誤解を招く大きな要因です。
次に、セマンティックですが、この文章の中には、4 つの「センサ」が出てきます。「水量に関するセンサ」については、「水位センサ」のことなのか、「水位センサ」と「満水センサ」の両方を示しているのか、あるいは、別のセンサのことなのか曖昧さを感じられたことと思います。
この文書に対して、構文形式について文法を明確にし、セマンティックの曖昧さを排除すると、以下のように表現することができます。

「水位センサが ON かつ満水センサが OFF の場合、本製品は温度制御を開始します。水位センサと蓋センサの 2 つが OFF の場合、本製品は温度制御を停止します。」

このように、仕様や設計に曖昧さがあると、誤解釈によって製品に不具合を混入させてしまうことに繋がりかねません。それでは、このように誤解のない表記を実践するためには、何をすればいいのでしょうか。

開発プロジェクトでは、前提知識や経験の異なる組織内外の様々な関係者との情報伝達が行われます。その際、相手の前提知識や経験によって、自分が常識と思っていたことが正しく伝わらなかったという経験をお持ちではないでしょうか。
実際、製品に混入する不具合には、要件や設計内容の誤解釈に起因するものが少なくはありません。
この誤解釈を低減するためには、「正しいことを正しく伝える」ための表記法が「共通の理解を得る仕組み」として存在する必要があります。前述の構文形式については、ガイドラインや手順書、セマンティックについては、それを統一するための用語集、テンプレート、ツール、さらにレビューに用いるチェックリストなど、「要件や設計内容が正しく解釈される仕組み」が必要になります。これらの仕組みを、組織内で表記法の共通認識として定着させるためには、関係者が仕組みを学ぶための教育や仕組みが定着していることを確認する監査も必要になります。
(2012 年 06 月臨時号 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