DNV·GL

DNVGL WHITE PAPER REGARDING SAFETY AND SECURITY

IEC TR 62380 は廃版なので利用できないのか？

Report No.: DNVGLS&S-WP-001, Rev. 1.0
Date: 2021-2-10

Table of contents

1　定量的安全評価がなぜ必要か

故障率データベースについてお話をする前に、故障率を用いた定量的安全評価がなぜ必要なのかを再度確認してみましょう。ISO 26262 における定量的安全評価の目的はなんでしょうか?　アイテムにおける残存リスクが 10 FIT や 100 FIT を超えないことを保証することでしょうか？　必ずしもそうであるとは申せません。ISO 26262 ではリスクが十分に制御され抑制されていることが求められます。それはすなわち、アイテムの識別されたハザードに関わる残存リスクの絶対値が許容リスクを超えないようにするというよりも、むしろ、残存リスクについて、従来の十分に実績のあるアイテムと比較することで、新たに設計されたアイテムが妥当な安全性を有していることを示すことにあるように思われます。

1.1　フォールトツリー分析の目的

皆さんは定量的に残存リスクを評価する上でフォールトツリー分析を実施されると思います。フォールトツリー分析の目的は何でしょうか?　多くの方が、PMHF の算定とお答えになると思います。確かにそれも誤りではありません。しかしながらフォールトツリー分析の真骨頂は、算定された数値ではなくフォールトツリーによって構造化されたリスクの内訳（ミニマルカットセット）です。すなわち、ハザードに至る意図機能の故障モードと安全機構の組み合わせにおいて、どこにハザードへの有意な影響があるかを識別することです。

これに関係する要素は大きく分けて 3 つです。

1 つ目はフォールトツリーの構造：すなわち当該の故障モードがフォールトツリーの上でどのように位置するのか；OR ゲートの下にあり直接ハザードをもたらすのか、AND ゲートにおいて安全機構に保護されているのか？

2 つ目はカバレッジ：意図機能が安全機構で保護されている場合、安全機構によって意図機能の故障モードがどの程度の割合で保護されているのか？

3 つ目が、意図機能の故障モードや安全機構の故障確率に関わる故障率です。

したがって、故障率データベースは、先に述べた定量的な安全評価の目的やフォールトツリー分析における故障率データの役割を鑑みて選定する必要があると言うことです。

1.2　安全分析における故障率データベースの役割

安全分析の目的がアイテムの新旧比較、つまり先のアイテムの実績をベースとした安全妥当性の確認であるならば、新旧のアイテムの定量評価において故障率データベースを取り替える事は適切ではありません。何らかの理由によって故障率データベースを置き換える必要が生じたとしても、できる限り従来と同じように故障率を扱えることが重要です。なぜならば、故障率データベースを取り替えることによって、故障率の数値や故障率の算定に関わる故障モデルが変わった場合、PMHF の値もその内訳も変わるため、アイテムの新旧比較による安全妥当性の確認が困難になるからです。
従って、よほどの事情がない限り、定量評価のベースとなる故障率データベースは取り替えない方がよいと言うことです。

2　故障率データベースの変更を余儀なくされた場合

しかし、何らかの事情によって、故障率データベースの変更を余儀なくされた場合、例えば IEC TR 62380 が廃版になったことに対して、どのように対処すればよろしいのでしょうか？　まず、故障率データベースを直ちに他のそれに置き換えることは推奨できません。

ある程度の期間、新旧 2 つのデータベースを併用することで、データベースの相違に関わるメトリックやフォールトツリー分析に現れる影響を把握することが肝要です。ISO 26262 2nd ED の Part 5 では、廃版になった IEC TR 62380 への参照が削除されておりますが、Part 11 では、おそらく上述の観点もあって、旧 IEC TR 62380 の説明にかなりのページが割かれております。

3 故障率データベース置き換え時の留意点

それでは故障率データベースを置き換える場合、どのようなことに留意すればよろしいのでしょうか？ ここでは、旧 IEC TR 62380 から、シーメンス社の故障率データベースである SN 29500 に置き換える場合を想定してお話いたしましょう。まず、従来用いていた故障率データベースである旧 IEC TR 62380 と SN 29500 の特質の違いを理解することが肝要です。特質と言うのは故障率の数値のことだけではありません。むしろ、重要なのは故障率の算定において想定されている故障モデルの違いです。例えば、故障モデルにおける稼働時間と非稼働時間の扱いの相違。あるいは、半導体のダイとパッケージの扱いの相違です。

まず、稼働時間と非稼働時間について申せば、SN 29500 では稼働中の故障率しか考慮しておりません。これに対して、旧 IEC TR 62380 では半導体のダイに関して、稼働時間と非稼働時間の割合を考慮することで両者のもとでの温度に関わる故障率への影響を平均化しております。ISO 26262 における PMHF の算定においては、原則として稼働中のリスクを考えるため SN 29500 を用いる、もしくは旧 IEC TR 62380 において非稼働時間を 0 と設定する評価が保守的です。しかしながら、わが国においては 旧 IEC TR 62380 を用いる際、そこに掲載されたサンプルのミッションプロファイルがそのまま利用されることもあり、このプロファイルに従って稼働時間と非稼働時間が設定されることも少なくありません。つまり非稼働時間を設定することで、稼働中のそれと比べて故障率を低く見積もる結果となります。これは必ずしも正しい方法とは申せませんが、新旧比較が定量評価の目的であることを鑑みると、この扱いを直ちに改める事も適切ではありません。仮に SN 29500 を用いることになったとしても、これまで同様、稼働時間と非稼働時間の比率を考慮することが適切です。先に申した通り SN 29500 では、基本、稼働中しか考慮しておりませんが、ストレスファクターのパラメーターを利用して稼働時間と非稼働時間の比率を反映させることができます。このようにして、異なる故障モデルをすり合わせるやり方をハーモナイゼーションといいます。JasPar では、故障モデルに IEC 61709 を、そこで参照されるリファレンス故障率に SN 29500 を用いるケースを検討しておりますが、考え方は同様です。
（JasPar：「ハードウェア故障率ガイドライン」2020.12 ご参照）

もう一つの重要な違いとして、 旧 IEC TR 62380 では集積回路の「半導体のダイ」と「パッケージ」を異なる故障モデルで評価しているため、両者の影響を分けて算定することができ、結果として、パッケージ側の故障率を半導体のピンの故障に按分することが可能です。これに対して SN 29500 ではダイとパッケージを識別して評価しないため、ピンへの故障率の按分ができません。それ故、個別のピン故障を鑑みた定量評価が困難になります。このことについては、ISO 26262 の Part 11 でも触れられておりますが、故障率に関するダイとパッケージの比率を旧 IEC TR 62380 から借用し、 SN 29500 に適用する方法などもあろうかと思います。

4 最後に

故障率にはある程度の精度が必要ですが、それは、定量評価の目的であるアイテムの新旧比較やミニマルカットセットの重み付けに必要とされる「相対的な」精度です。つまり、故障率の絶対値に固執するよりも、スケーリングやハーモナイゼーションを踏まえた、故障率データの継続的な一貫した取り扱いの方がより重要であると申せましょう。

About DNV GL

DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.