JCMA 報告

ISO/TC 127（土工機械）/ WG 11（ISO 15998 適用指針）ストックホルム国際会議報告

標準部会
ISO/TC 127 土工機械委員会

1. 経緯

電子制御が土工機械分野でも普及していることから，長年の審議を経て ISO 15998（土工機械－電子機器を使用した機械制御系（MCS）－機能安全のための性能基準および試験）が正式に公布されたが，IEC 61508 シリーズ（= JIS C 61508 シリーズ“電気・電子・プログラマブル電子安全関連系の機能安全”）他，多くの標準を引用しており，特に IEC 61508 は難解で分量も多く，多くの手法や推奨が提示されていて具体的にどのように適用したら適合するのかが判断しづらい状態である。このため，実際に ISO 15998 を製品開発に適用するといっても各メーカの考え方および適合を審査判断する各種機関の考え方が必ずしも一致するとは限らない。そこで ISO 15998 に適合していると判断される具体的な実施内容の例を策定し，これを指針として各メーカが大きなばらつきなく ISO 15998 を適用した製品開発ができるようにすることを目的として，TS 11585（ISO 15998 適用指針）を開発のため ISO/TC 127/WG 11 が設定され，第 1 回国際会議が本年 4 月にストックホルムで開催された。

2. 会議場所など

・日　時：平成 20 年 4 月 14 日，15 日
・場　所：スウェーデン国ストックホルム市
・出席者：米国 6 名（John Deere 社より 2 名，Cat 社 1 名，Bobcat 社 1 名，Vermeer 社 1 名，Ditch Witch 社 1 名），ドイツ 1 名（Liebherr 社），スウェーデン 2 名（Volvo 社 1 名，Dynapac 社 1 名），英国 1 名（JCB 社），日本 1 名（コマツ）。全てメーカの人で，ISO 15998PL で担当の SC 3/WG 2 コンビナーのドイツ DGUV の Dr. Schaefer は欠席　計 11 名
●TC 127/WG 11 コンビナー（主査）：Mr. Gamble（米国，John Deere）

3. 概要

米国は ISO 15998 策定の過程で IEC 61508 が参照されていることに大きく反意を示していた。しかしこれが制定されたということで，国内のメーカで集まり，真っ向から IEC 61508 を分析し，解釈し，どのように適用すべきかをワークしている。そのワークの方向性および成果を最終的にガイドラインとして国際規格化しオーソライズしたいという意志があり，まだかなり不完全ではあるが，ドラフトを作成した。そもそも ISO 15998 は IEC 61508 以外にも手法等は選択の自由があるが，PL 訴訟等では自社の判断で行ったことで戦うことは無理だと考えていることが背景にある。以上のように米国の真意および姿勢は至極まじめなものであり，弊職は IEC 61508 にあまりに正面から立ち向かいすぎていると感じた。

JCB および Volvo は部分的ではあるが IEC 61508 を適用する方向で分析や設計を始めているが，解釈や実施内容はばらつきが大きく，欧州としての定説ができてはいないことが判明した。

弊職は当初から IEC 61508 以外の方法で ISO 15998 に適合すれば良いと考えていたが，欧米各社の状況および方向性から，このまま進むようであれば，日本のメーカも諸外国と同じ路線を踏襲する必要があると判断する。また，欧米各社の方向を変えるという選択肢を取ることもあり得るが，その場合，PL 訴訟でどのようなことになるかを説得性ある形で提示しつつ提案しない限り難しいと判断する。

会議では，実際の IEC 61508 を適用して，リスクアセスやそれによって導出される安全度水準（SIL）の決定，さらに要求される安全度水準を実現するための証明方法や二重化等の信頼性向上の手段等を一連，実施してみた。結論として，やはり皆が合意できる統一した IEC 61508 の解釈の仕方および適用方法は得られなかった。大きな課題は，以下に示す。

1）リスクアセスは C（Consequence：被害の大きさ），F（Frequency：危険への露出頻度），P（Possibility：危険な事態の発生確率），W（Possibility of unwanted occurrence：好ましくない結果の起

こる確率）にて SIL 値を定めるが，W についての解釈が他業界も含め現実に先行する欧州でも諸説あり確定せず。これ如何で結果が大きく変わり得るため，統一した解釈とそれぞれのパラメータの具体的程度が建機業界に必要（いずれも数値の大きい方が危険側）。

2）建機の機種毎のどの機能が誤動作し，事故が発生し，被害の程度が仮定できた場合，それは世間の他業界の経験や常識から見てどのような安全度水準 SIL 値であると理解されるかが不明。すなわち上記リスクアセスの結果から導出される SIL 値は，他業界等と比べて十分に不足のないものとならなくてはいけない。

3）求められている SIL 値を実現したと言えるための手法に様々なものがあり，実際にどこまでやったら建機では十分やったと言えるかが不明。例えば航空機のように厳密な故障確率を求めたり，信頼性を高めるために 3 系統のシステムを並列に持ち，2 系統以上の結果の一致を見て制御をする等が建機でも必要か否か。

4）以上のようなことに対して参加メンバーでは結局，解が求まらず，次回はドイツ DGUV の Dr. Schaefer の解説および判断が必須ということになった。事前のワーク等のリストアップとアサイメントを実施して，次回は Dr. Schaefer のお膝元 Sankt Augustin, Germany で 9 月 8 日から 2 日間の WG を開催することになった。

5）日本（コマツ）が受けた（立候補）事前の宿題のうち大きなものは，油圧ショベル（クローラ式，タイヤ式）のリスクアセスを IEC 61508 の方法で実施してみることである。

4. 主要議事

4/14　自己紹介後，各自が今回の WG に対する期待を表明。課題意識は同一で，WG に対して肯定的。ドイツから ISO 15998 開発担当の TC 127/SC 3/WG 2 コンビナーが来ていない。諸事情で来られなかったようである。よって，ドイツはメーカから 1 名のみで彼がドイツを代表する。メーカのメンバーはほとんどが規制規格の担当。エレクトロニクスの専門家は少ない。

IEC 61508 は本当に解釈が難しい。確率が実務で本当に使えるか疑問。

2oo3（2 out of 3：三つ並列システムのうち二つ有効な結果を使う）は Volvo の Bergsten 氏の経験では軍用航空機位しか使わない。等々，課題意識は大体一致。主な論議としては：

1）リスクアセスの W（好ましくない結果の起こる確率）の意味について議論，経験がある場合は W1，ない場合は W2 という案や，自社内のシステムなら W1，他社のものなら W2 など諸説いろいろあり。Volvo の Bergsten 氏が調査しただけで，4 通りの解釈が世間にあるとのこと。全くよくもこんなものを IEC にしたものだと思う。結論は出ず。

2）JCB の Andy は英国で quantitative な方法（故障確率使用）を使っているということで，自社でやっているやりかたで確率を算出する例を紹介。10E-5 という許容できる年間の死亡確率（通常の人が病気や事故等で亡くなる確率と同等）からスタートし，これを「failure が起こっても fatal に至らずにすむ確率」で割る。そうすると許される failure の確率が出るはずである。よって，システムはこの確率以下の故障率を持つ程度の信頼性で作られていれば良いということになる。

これで，公道を走る高速車がギアダウンして後続車を事故に巻き込んで fatal になるという想定で確率を求めたら，安全度水準 SIL4 レベルが要求された。これはおかしいということになり，シミュレーションとして fatal に至らずに済む確率をいじっても，SIL2 どまり。うーん，難しいということで，午後はリスクアセスから典型的な SIL を求めてみようということになった。

公道走行があり，比較的高速なローダを例にリスクアセスをやってみる。

3）ローダが静止状態で突然動き出す場合

ローアイドルの車に乗っているオペのリスクに着目。

C1，F2，P1（C：被害の大きさ，F：危険への露出頻度，P：危険な事態の発生確率）で一致。ところが W の解釈で再び紛糾。W の意味が定まらず。これでは先へ進めないので，取りあえず W には W1 と W2 の両方のケースでアセスを進めることにした。崖っぷちを高速で走っているときや公道で走っているとき等を加えても，propel に関しては，SIL1 が最も高いことになった。

4）次は公道でステアが無くなる

結果は W1/W2 で SIL2/SIL3

5）公道でブレーキが無くなる

結果は W1/W2 で SIL2/SIL3

6）稼働中にバケットやアームが動く

結果は SIL1

以上のように，建機ではものによって，SIL1 から

SIL3 までが出てきそうなイメージで，SIL4 はない。これはメンバーもその程度だろうという認識で一致している。

休憩を利用して個人的に秋から始まる EN 474 で要求される ISO 15998 対応方法を JCB の Andy に聞いた。結果は，以下のとおり。

既存の 200 機種以上のものに新たに対応をすることは新しい開発を止めることを意味している。そんなことはできない。よって，対応は既存の社内の仕組みが ISO 15998 に照らして適合しているという方法で行う。

4/15　建機では SIL1 ～ SIL3 程度があり得るという前提で，では実際にそれらの SIL を実現するとはどういうことかという観点で議論をする。

John Deere の Rick が 1oo1 は SIL1 に十分かという議論を始める。

メーカとしてはこのような紐付けができれば非常にありがたいのであるが，所詮 SIL 値が要求していることはシステムが期待通り動いてくれるという機能率につき，定性的には何か関係がありそうだという直感の域を出ず，1oo1 が妥当であるという証明は苦しい。

IEC 61508 の提唱するひとつの方法は，Safe Failure Fraction（故障しても安全な確率）を計算して，IEC 61508 の中で SIL 毎に決められた表の値と比べて合致しているか判断する方法があることが紹介された（IEC 61508-2 table2，table3）。

ISO 13849-1 には SIL に近い概念であるカテゴリー分け毎に 1oo1 等のアーキテクチャが載せられているという紹介はあったが，議論の進展はなし。

結局，SIL 毎の generic なアーキテクチャのリコメンデーションを作りたいが，簡単にはできない。Dr. Schaefer に是非このようなやり方が妥当であるか，またその場合の対応付けはどのようなものなら納得できるか是非聞いてみようということになった。

ハードウェアは故障率で信頼性を証明するが，ISO 13849-1 Annex C には複雑な MTTF や B10 等の算出の仕方の表があることが紹介されたものの，これをどうするという議論にはなっていない。

IEC 61508 の考え方では，複雑なシステムやプログラミングの部分については，故障率で議論することは難しいので，開発のプロセスや道具立て，組織や検証の仕方等で信頼性を確保する。これについては，現時点（IEC 61508 が制定された時点）で有効とされる膨大な技術が列挙されているが，ソフトの専門家として弊職にコメントを求められた。列挙されている内容はある意味常識的なものもきちんとあり，妥当なものも多いので，理解はできる，さほど問題ないと答えた。ただし，ここまでは言及しなかったが，メーカは実際にどれをきちんとやっていると後で証明するのは非常に難しいと感じる。これについてはメーカ毎に実際に採用している技術は千差万別であろうが，肝要なことはどれを適用しているときちんと明示すること，およびその適用のエビデンスを残すことであると解釈している。

以上

文責：中野　一郎（コマツ　システム開発センタ）

JCMA