部　会　報　告

ISO/TC 127（土工機械）/SC3（機械特性・電気及び電子系・運用及び保全）/WG 8（ISO 15998 適用指針）ドイツ国際会議報告

標　準　部　会・ISO/TC 127 土工機械委員会・中野　一郎（コマツ）

1. 概要

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及び試験」が 4 月に正式に公布されたが，これは IEC 61508 = JIS C 0508 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，多くの標準を参照している。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るため，具体的にどれをどこまで適用したら適合していると言えるかが判断しづらい状態である。したがって，現状のまま実際に ISO 15998 を製品開発に適用した場合，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ことが懸念されている。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指針としてまとめ，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するために作業グループ（ISO/TC 127/WG 11）が構成され，今回は 4 月に続き，二回目の会議となる。なお，この案件は 5 月に開催の ISO/TC 127 総会で TC 127 傘下の SC 3 分科委員会に割り当てられ，それに伴い作業グループも SC 3 に移管されて SC 3/WG 8 となり，また案件の番号も当初 ISO/T 11585（TS は ISO 規格と比べて合意のレベルの低い ISO の技術仕様書）とされていたが，今後は IS 15998 との関連のため，その第 2 部となる見込みである（未手続き）。

2. 会議場所など

・日時：平成 20 年 9 月 8 日～ 9 日
・場所：ドイツ国（ボン近郊）ザンクトアウグスティン市 BGIA（Berufsgenossenschaftliches Institut für Arbeitsschutz（ドイツの労働災害保険機構の連合体 HVBG - Hauptverband der gewerblichen Berufsgenossenschaften（German Federation of Institutions for Statutory Accident Insurance and Prevention の研究所）にて
・出席者：米国 5 名（Cat 社 2 名，Vermeer 社 1 名，Ditchwitch 社 2 名），ドイツ 1 名（Liebherr 社），スウェーデン 2 名（Volvo 社，Dynapac 社），英国 1 名（JCB 社），日本 2 名（コマツ）。メンバーは全て建機メーカの規制標準担当もしくは開発担当者。また，ISO 15998 コンビナーであったドイツ BGIA の Dr. Schaefer が部分的に出席。　計 12 名
・TC 127/SC 3/WG 8 コンビナー（WG 主査）：David GAMBLE 氏（米国，John Deere 社）

3. 主要議事

重要な進展または決議は以下の通りであり，日本としては望ましい方向で問題なく進展したと考える。

1）リスクアセスの方法およびパラメータの解釈が確定

ISO 15998 Annex A には IEC 61508-5 Annex D より引用したリスクグラフによるリスクアセスの方法が紹介されており，指針では引き続きこれを使用するが，曖昧であった各種パラメータの解釈が確定した。

-Frequency パラメータに対しては F1 と F2 の境界を 10 %の頻度と考える。

-W パラメータについては Dr.Schaefer に確認した結果，結局定説はないということで，指針としては一律 W2 を使用することとする。

2）各種建機のリスクアセス

日本の提案により，油圧ショベルは建機の台数から見ても大きいため，まずはリスクアセスの例として油圧ショベルを固めることとし，主要な生産国である日本がエキスパートとして次回に向けてリスクアセス結果を提案することとした。

3）システムに要求された SIL（安全関連系に割り当てられる安全機能の安全度要求事項についての水準で 1 が最低，4 が最高）を満たしていることを証明する方法

IEC 61508 ではハードウェアの偶発故障率等の信頼性を定量的に保証することが求められている。化学プラント等の安全装置等では部品の故障率等のデータがデータベース化され，定量値を求めるためのインフラ

が進んでいるが，建機や自動車等ではこれらが現状不十分。よって，定量的（quantitative）な保証だけではなく，定性的（qualitative）な保証でも良いとすることで指針を作成することを再確認した。

ハードウェアの故障については，定性的な保証の方法をドイツが次回提案する。

ソフトウェアの信頼性確保やハード＆ソフト開発のプロセス管理等についての定性的な保証の方法についてはスウェーデンが次回提案する。

4）権威である Dr. Schaefer の重要なコメント

現在の WG のメンバーである各国の建機メーカは，最も建機業界の知識と経験を持つ権威者として認めることができるため，WG にて合意を得ればそれを指針として策定することは問題ない。

定性的な保証ということもあり得るが，将来的には定量的な保証を望む。現在，EN 954-1 Safety of Machinery とハーモナイズされた ISO 13849-1:2006 があるが，機械に適用するには IEC 61508 よりこちらが適当である。この ISO は定量的な保証を求めている。

5）次回の予定

来年 4 月 21 − 22 日を次回の WG とし，Dr. Schaefer が参加し易いようドイツで実施する。

4. 詳細事項

1）案文 TS 11585 に対する各国コメントとその対応審議のうち，特筆すべき事項

a）指針の案文と ISO 15998 の関係（置き換えか補填か？）がはっきりしないため，日本よりこれを正すために問題提起を実施し，結果として案文は ISO 15998 と共に使用する補填であり，ISO 15998 の部分を引用するような内容重複は避け，必要があれば参照とすることになった。

b）ISO 15998 および今回の指針案文の方針として，必要な SIL を実現するにあたり，定量的な信頼性を求めて証明する方向を取るのか，定性的なもので OK とするのかをまず定めるべきという日本からの問題提起を実施した。

さらに日本としては，建機では定量的な手法はまだ実施に困難が予想されると思われるので，定性的なものを OK とする方向で進めたいと進言した。事実，現在入手しているや自動車の機能安全に向けての ISO/CD 26262 では，定量的な目標値が informative になっている。これに対して即座にドイツ（Liebherr の Knecht 氏）が定性的なものを OK とする方向に対して賛同を表明。

ただし，定性的なものを認めるとしてもメーカとして何をもって必要十分なことをやっていると言えるかについてはまだまだ曖昧であり，既存の IEC 61508 等を参照しても問題は解決しないということで，以下の分業を実施することになった。

ハードウェアの故障については，定性的な保証の方法をドイツが次回提案する。

ソフトウェアの信頼性確保やハード＆ソフト開発のプロセス管理等についての定性的な保証の方法についてはまずは SIL 1 を対象にスウェーデンが次回提案する。

これらの成果により，案文の IEC 61508 から部分的に引用した Table 1 および Table 2 は書き換えられるはずである。

c）リスクアセスメントの指針を Annex A に示し，これにより具体的な建機の各機種がどの程度のリスクを持ち，その結果どの程度の SIL を要求するかを一般論として示そうとしている。ISO 5998 Annex A では IEC 61508-5 Annex D より引用したリスクグラフによるリスクアセスの方法が紹介されているが，指針でもこれを使用することとしている。しかしこのリスクグラフで使用する各種パラメータ C，F，P，W の解釈と用法が曖昧であったため，それらについて審議し，下記の結果となった。

Frequency に対しては F1 と F2 の境界を 10 %の頻度と考える。

W については一律 W2 を使用することとする。

d）初回の WG でも話題になったが，指針では求められる SIL を実現するための典型的なハード構成（アーキテクチャ）を定めるべきという要望がある。それにより，何が何でも航空機やロケットのようにコンピュータを三台積んで，多数決で結果を決めるような，建機や自動車では現状とかけ離れた構成を採らねばならないような誤解を防ぐ必要がある。

案文には IEC 61508 をベースにしたアーキテクチャの例とその得失を Annex C にまとめようとしてあるが，現状では間違いや過不足が目立つので，日本がこの部分の修正案を作ることとした。

2）Dr. Schaffer との意見交換

ISO 15998 および本案文策定作業では，ドイツの公的労災保険の機構に勤める Dr. Schaffer を活動の方向

性を相談する権威者と位置づけてきた。

彼によるとISO 15998作成時点ではIEC 61508もしくはその他類する標準等を多く参照することになったが，今作り直すとすると全く異なったものとしたく，基本はISO 13849を使ったものになるであろうとのこと。よって，ISO 13849についてより良く知って欲しく，別途BGIAよりプレゼンを実施することになった。

ISO 13849は2006年に改訂され，IEC 61508やIEC 62061では不十分であったところが改善され，EN 954-1 Safety of Machineryとハーモナイズされたため，機械に適用するには現在最適なものとなっている。

ただし，Dr. Schafferは現在までの活動を転じてISO 13849-2006を使用するようにとは言わず，WG活動に参加している各国の建機メーカは，最も建機業界の知識と経験を持つ権威者として認めることができるため，WGにて合意を得ればそれを指針として策定することは全く問題ないと認めてくれた。

また，リスクグラフのwパラメータについては，過去にも多くの議論があり問題であることを認識していて，個人的にもこのようなパラメータの導入は嫌いであり，ISO 13849のリスクグラフの手法では排除をしたそうである。

3）定量的リスクアセスの紹介

Andy Williams（JCB）が「Quantitative Approach To SIL Target」と題してリスクグラフによる定性的なSIL決定法に対して，定量的なSIL決定法をプレゼンした。

前回のWGで同様な内容を口答で説明しようとしたが，上手く行かなかったため，今回はそれをきちんと資料にまとめてきた。

荒筋は前回と変更無く，まず「failureが起こる確率」が判り，そのfailureが起こった前提で「fatalな事故になる確率」が判れば，両者を掛け合わせたものが「fatalに至るfailureが起こる確率」が判る。この「fatalに至るfailureが起こる確率」を充分に許容できる数値以下に抑えるように「failureが起こる確率」を小さくする，すなわち必要十分に高い信頼性のシステムを作ると考える。ここで十分に許容できる数値としては，10 E − 5 per yearという確率（通常の人が病気や事故等で亡くなる確率と同等）を使用する。なお，この確率は歩行者等，敢えて危険を冒しているという認識を持たない人に適用する。オペレータのように自らの選択がある場合は，一桁大きい確率を適用する。

詳細は省略するが，「fatalな事故になる確率」を求める部分はシナリオを立て，これの局面毎に確率を決め，それらの総積を使用する。しかし，確かに確率という定量値を使ってはいるが，シナリオの立て方や局面の確率値の求め方は甚だ定性的であり，結局リスクグラフのC，F，P等のパラメータを使うことと大差ないと感じた。

上記の方法で，許容される「failureが起こる確率」が決められるため，これからIEC 61508の対応するSILが判り，それが最低限実現しなくてはならないレベルとなる。では，そのレベルを実現すればOKかというとそうでなく，ALARP（As Low As Reasonably Practicable）という「合理的で実践的な限りできるだけリスクが低くなるよう」システムを作る必要があるという。このALARPの概念にも定量的な計算があり，救える人命をコストで換算し，システムを改良するコストと比べ判定するという方法が紹介された。これについては，米国では弁護士がこれを知ったら必ず裁判で乱用するということで米国からは強い反意が出た。ただし，これらは指針に入れるという提案ではなく，JCBからの英国で行われている手法の紹介である。

さすが，保険を発明した国らしく，定量的な計算が好きなようだが，まじめにものを改善する側に努力を傾倒する日本の文化から見ると，やらない言い訳を如何にエビデンスとして残すかに努力を使っているように感じる。

AndyはResearch部門所属で，Electronics and Control SystemsのManager。開発実働部隊の方向付けを行っているという。Andyに直接尋ねると，本プレゼンは現在社内でやろうとしている方向を示していて，まだ完全に開発に適用しているとは言えないようだ。

4）IEC 61508より実践的なISO 13849の紹介

DGUVのMichael Hauke氏より「A Practical Standard to Evaluate Control System for Safety（IS 13849）」という表題で，EN954-1 Safety of Machineryとハーモナイズされた ISO 13849-2006の内容について紹介された。

制定が古く適用範囲が広いIEC 61508より，機械に適用するにはこちらが適当であり，複雑な計算をせずに簡略化された手法もある。ただし簡略化されたものは安全サイド側の判断が出るようになっている。

また，併せてBGIAにて開発されたISO 13849の手法で計算してくれるソフトウェアツールも紹介された。

5）油圧ショベルのリスクアセス結果

前回のWGミーティングにて，JCBがバックホーローダ，CATがグレーダ，コマツがクローラおよびタイヤ式油圧ショベルのリスクアセスを宿題として実施することになっていたが，やってきたのはコマツのみ。

内容を簡単に説明した。なお，米国が用意したTS 11585の案文中にあるSILレベル例を挙げた表は最高でもSIL 1となっているのに対してコマツ案は公道走行時のステアで一部SIL 2としている点が異なる。なお，このリスクアセスはwパラメータの使い方が決まる前に実施したものにつき，見直しが必要である。

日本の提案により，油圧ショベルは建機の台数から見ても大きいため，まずはリスクアセスの例として油圧ショベルを固めることとし，主要な生産国である日本が次回に向けて再度リスクアセス結果を提案することとした。

また，TS 11585の案文中にあるSILレベル例を挙げた表について，次回までに意見があれば出すことになった。

以上

JCMA