部　会　報　告

ISO/TC 127/SC 2/WG 24（ISO 19014 土工機械―制御システムの安全）2015 年 5 月スウェーデン・ストックホルム市 国際作業グループ会議報告

標準部会 ISO/TC 127 土工機械委員会国際専門家（Expert）
田中　昌也（コマツ）

2015 年 5 月に国際標準化機構 ISO の専門委員会 TC 127（土工機械）傘下の国際作業グループ ISO/TC 127/SC 2/WG 24（ISO 19014 土工機械―制御システムの安全）会議がスウェーデン国ストックホルム市で開催され，協会標準部会 ISO/TC 127 土工機械委員会から国際専門家（Expert）として出席した田中昌也氏の報告を紹介する。

会議：ISO/TC 127/SC 2/WG 24 国際作業グループ会議

1　**開催日**：平成 27 年 5 月 11 日（月）～ 13 日（水）

2　**開催地**：スウェーデン国ストックホルム市 SIS（スウェーデン規格協会）

3　**出席者**：15 名

米国コンビナ（主査），Part 2 プロジェクトリーダ，Part 3 プロジェクトリーダ，他 4 名
英国 Part 1 プロジェクトリーダ，他 2 名
日本 1 名
スウェーデン 2 名
ドイツ 1 名
英国 2 名
イタリア 2 名
オーストラリア 1 名

4　**議題及び経緯**：

Part 1: Earth-moving machinery - Safety - Risk assessment methodology to determine control system performance requirements
Part 2: Earth-moving machinery - Safety - Design and Evaluation of Safety-Related Electronic Machine Control Systems
Part 3: Earth-moving machinery - Safety - Environmental Testing

建機の機能安全規格として 2008 年に ISO15998-1 が制定済みで，その適用ガイドライン ISO/TS15998-2 が 2012 年に制定された。しかし，多大な苦労を重ねて作成した ISO/TS15998-2 をもってしてもリスクアセスメントの「だれが何度やっても同じ結果になる」は達成できておらず，早々に改定提案が出され，その 6 回目の会議。

ヨーロッパ開催であるが，ひやかしで出ている感じの人は来なくなり，出席人数が落ち着いてきた。

公式議事録：ISO/TC 127/SC 2/WG 24 Doc N 91

◆決定事項：

・現在標準トラック（36 ヶ月で規格発行）であるが，日程的に無理なので，延長トラック（48 ヶ月）に変更する。そのうえでさらなる期間延長のため自発的キャンセルを行い，そこからの再開方法を次回会議（2015/12）において決める。
・ドラフトの作成を加速するため，特定のテーマを検討する Ad Hoc Group を結成し，その Ad Hoc Group が担当部分についての原案を作成する。
・AHG 1「リスクグラフの妥当性検討」及び AHG 2「コントローラのソフト・ハードへの要求検討」の 2 つの Ad Hoc Group が結成され，報告者は両方に参加する。
・AHG 2 のメンバーは Doc N 86 に対する意見をソフト・バス通信部分担当予定のイタリア専門家に送付する。
・次回会議予定
2015/12/7 @ ロンドン。これが通常の WG 会議で，それ以前に Ad Hoc Group 会議として，AHG 1 が 2015/8/17-21@ 米国ピオリアで予定されている。AHG 2 は調整中。

◆所感：

・「ISO 13849 をベースに，一部 IEC 61508（又は他規格 ISO 25119）の考えで補強する」というコンセンサスが感じられ，大局的には無意味に厳しいものにはならないと考えられる。今回まで残っているメンバーは知識のレベルがかなり上がってきており，会議はスムーズに進んだ。

◆議事メモ：

Part 1

・リスクアセスメント手順と PLr（制御システムに要求されるパフォーマンスレベル）の決定まで英国プロジェクトリーダ（以下 PL）が担当。

PL が「コンセンサスがとれないので，ISO でなく TS（Technical Specification）にしては」と言い出したが，Ad Hoc Group に実務が振られ，そこで作業を進めることになった。PL がベースにしようとしているリスクグラフ（リスクグラフについての投票結果を加味したもの）は，一見したところ今回の会議前に配布されたドラフトから，更に厳しめになっているようなので，修正は必至と思われる。

Part 2

・実際に設計した制御系を評価して PL（達成されたパフォーマンスレベル）を算出する部分で，米国 PL が担当。

・電気以外の動力源（油圧や空気圧）を使った制御系の扱いについて

電気電子を使用しない制御系（オービットロールのステアリング等）。メカ部品は全部 exclude してよい（MTTFd 計算しなくてよい）ことにしようとの提案があったが，WG の議論では全部 exclude するのは不可となった。

制御入力から制御出力までが対象範囲で，それ以外の構成品は exclude してよい。

また，対象となる部品に対して認められる fault exclusion（条件を満たせば MTTFd の計算から除外してよい故障モード）を明確にしてドラフトを作成し，これに対しコメントを提出することとなった。

電気・電子を使用しない制御系に MTTFd=Very High という分類を追加することで，カテゴリ 2 で PL=d，PL=e を実現できることにする。この場合，TE はシャットオフバルブ程度で良いことにする。

・機能安全達成度合の名前

MPL（Machine PL）にするか，PL（ISO 13839 の尺度）にするか？ →とりあえず MPL でいく。名前を変えるのは，要求事項が ISO 13849 と違うため。但し，MTTFd（危険側 MTTF）だけに限って言えば，MPL=PL である。ドラフトも PL のままなので，本報告でも PL で記述する。

・ソフト

ISO 13849 には PL に応じたシステマティック故障（ソフト含む）の手法選択がない。ISO 25119 にはあるので，それと揃えてはどうか？（イタリア専門家）

PLC（いわゆるシーケンサ）についても記述する（米国専門家）。

イタリア専門家が，非常によくできた規格間の対比表（Doc N 85，N 86）を作ったので，これをベースに Ad Hoc Group で検討を行う。

Ad Hoc Group で詳細の検討が始まるので，ドラフトの厳密なチェックが必要である。

Formal Method（形式手法）について，どういうものか WG メンバーの誰も分からないのであれば除外しよう，という提案があった。

・ブロック法

PL=c のブロックと PL=d のブロックを結合した場合，達成できるのは PL いくつか，という問題。ISO 13849 に規定がある。また，IEC 61508 にも規定があるので双方を引用する。IEC 61508 からの引用について，正しく引用しているか（前提を理解しているか）調査要。

・“Simplified procedure for estimating PL”（7.5 項）

ドラフトに“Simplified procedure for estimating PL”という項はあるが「simplify されていない本来の手順」（という項）が無いので，その旨 前々回会議（2014 年 11 月）の前に報告者がコメントを提出した。前回会議（2015 年 1 月）で，そのコメントにつき説明を求められ，意図（simplified procedure があるなら non simplified procedure もあると誤解されるので，手法を 1 つしか用意しないのであれば，そうと伝わる表現にすべき）を説明したところ，「意図はわかった。ではどのような手法にしたいのか？」と聞き返され，報告者の宿題になっていた。

前々回（2014 年 11 月）の会議では，前プロジェクトリーダによる回答は「ベースとする ISO 13849 にも simplified procedure しかない。Non simplified procedure といえば IEC 61508 のことである」であった。報告者は，休憩時間中に「IEC 61508 をそのままやるのは本意ではない」旨を前 PL に話したが，それは理解したうえで「会議での議論の合意は IEC 61508 も（使いたければ）使えるようにしてほしい，ということだった」との回答であった。今回，ISO 13849 を改めて読んでみたが，前 PL の言っていたことが正しいと思われ「ISO 19014 は，Earthmoving Machinery に合った形で IEC 61508 を simplify するべきである。simplify の方法は，ISO 13849 にできるだけ合わせる」と提案して，概ね同意された。

・定性的解析のみによる PL の決定（Annex C）

→認められない。削除する。このような more simplified procedure とでもいうものが突然出てくるので，混乱を招く。

・通信バスにおける安全関連メッセージの通信（Annex I）

→ Part 4 へ。本文からの参照がない。対応する本

文が必要である。

・**制御システムの例と，それに対する PL 評価の例**（Annex J）
各国専門家・PL 達の宿題となった。特許で揉めるような図にはしないこと。または，特許部分を明示すること。

・**他の機能安全規格との互換性**（Annex K）
購入品をどう評価するか，が Annex の目的。購入品は ISO 19014 での PL（MPL）は規定されないと思われるため（SIL，ASIL，PL あたりが現実的か），換算方法を提供する。

・**ICT 建機の ICT 部分**（Annex L）
3rd party の製品が車体制御する場合を想定する。ICT 建機やステアリングを自律制御するような 3rd party 製品があり，そのような 3rd party へのガイダンスとなるが，要求については，未だ練れていない。会議参加者の発言を聞いていると，勝手に解析（“hacking”と言っていた）して制御を行っている 3rd party もあるようであり，欧州機械指令では（3rd party が二重に関わっているような場合），一番最後に手を加えた会社が責任を持つことになっている様子。

Part 3

・耐環境試験。米国専門家が担当。

・コメントは日本からの 1 件のみで，「温度サイクル試験の高温側を＋70℃で以上実施すること」との要求事項に対し，「キャブ内搭載前提のコントローラでは，そこまで温度が上がらない場合もあるので，設計の自由度を持たせるために除外すべき」と意見具申した。趣旨は理解されたが，今回の会議では結論を出さず，WG メンバーに対し「試験基準のミニマムの選び方について，次回会議までに再レビューしてコメントのこと」と宿題が出され，その結果とあわせて次回会議で審議されることとなった。

Part 4

・当初は Part 2 で電気・電子制御システムを扱い，Part 4 で電気・電子制御を使わない（油圧のみの制御システムなど）制御システムを扱う…という流れだったが，両者には意外と共通性があることが判ってきたため，むしろ共通部分を Part 2 にまとめ，電気・電子制御に固有なソフトとバス通信を Part 4 として分ける案が有力となってきた。