

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)
2017 年 3 月 米国イリノイ州ピオリア市 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)

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 2017 年 3 月に米国イリノイ州ピオリア市で開催され、協会標準部会 ISO/TC 127 土工機械委員会から前回 1 月に引き続き国際専門家 (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 29 年 3 月 27 日 (月) ~ 31 日 (金)

2 開催地: 米国イリノイ州ピオリア市

3 出席者: 17 名

米国 Part 2 プロジェクトリーダー, Part 3 プロジェクトリーダー, 他 10 名

英国 Part 1 プロジェクトリーダー

イタリア Part 4 プロジェクトリーダー

オーストラリア Part 5 プロジェクトリーダー

スウェーデン 1 名

日本 1 名

4 公式議事録: Doc N0164

5 決定事項

Part 1 (MPLr の割り当て) - DIS 投票のコメント処理とドラフトの修正が完了した。変更が多い為、FDIS でなく、第 2 次 DIS 投票 (DIS2) へ進む。

Part 2 (制御システムの実装と評価) - CD 投票に対するコメント処理の途中でプロジェクトを中断しているが、CD コメント処理の会議はこれ以上行わない。これまでの CD コメント処理の結果 (Doc N0163) が反映された WD (N0162) を添付して再開の投票 (NWIP) を行う。WG メンバは未処理の CD コメントで重要なものの再提出と、Part 2 を再スタートするにあたり必要なコメントを 4 月迄に提出する。

Part 6 (コントローラハードウェアの詳細設計への要求事項)

米国専門家が前任 PL 候補を引き継ぐ。6 月迄に案文を用意する。内容をレビューしたうえで Part 6 として独立させるか、Part 2 の Annex にするかを決める。

6 今後の予定

(投票)

Part 1 DIS2 (近々)

Part 2 NWIP (4 月)

Part 3 (耐環境性要求事項) FDIS (近々)

Part 4 (ソフトウェアへの要求事項) NWIP (3 月期限) 終了後, CD

(会議)

2017 年 5 月 Part 5 (ホイールローダ) @ スtockホルム

2017 年 6 月 Part 5 (履带式ショベル) @ 東京

2017 年 7 月 Part 2 @ フランス (フランス以降の開催地は予定)

イタリアで開催して CEN のコンサルタントを呼ぶ計画は調整がつかず、変更になった。

2017 年 9 月 WG24 全体会議 @ ロンドン

2017 年 11 月 Part 5 (バックホウローダ及びホイール式油圧ショベル) @ マイアミ

2018 年 1 月 Part 5 (アーティキュレートダンプ及びリジッドダンプ) @ オーストラリア

2018 年 3 月 Part 5 (スキッドステアローダ) @ ファーゴ, USA

7 日本のアクション

・Part 5 (Part 1 の実施例) は予想される作業量が膨大で、会議が多数計画されているが全てに出席するのは、準備も含めて困難が予想される。最初の 2 回の会議迄で内容のスリム化を図る必要があると思われる。

・オーストラリア PL のアセスメントによると、油圧ショベルの旋回が MPLr = e になるという話を以前から聞いているが、油圧ショベルの旋回のリスクが公道上を高速走行する車両のステアリングのリスクと同じというのは現実とかけ離れているのではないかと。Part 5 の油圧ショベルの会議を日本で開催し、油圧ショベルの専門家に多数参加してもらい、現実的なアセスメントを主張することにする。

・Part 2 には電気電子を含まない制御システムがスコープとして含まれるが、十分に市場実績のある油

圧システムを見直す必要は感じられず、油圧システムについて MTTFd や DC 等の計算をしたところで製品の改善につながらないのではないかという意見が大半であった。但し、規格として最低ラインは決める必要はあると思われる。

8 議事メモ

〈全体〉

- ・オーストラリア PL による Part 5 の提案に従えば、Part 1 に基づくリスクアセスメントに膨大な作業が必要になる為、多くの参加者から懸念が示された。
- ・米国専門家意見
ISO 13849 は基本的に産業機械やプレス機のような工場に据え付けて使う機械を想定しており、建設機械のアセスメントには適さない部分がある。また、ISO 13849 の次の改訂では、動き回る機械 (mobile machinery) を除外する予定であるという情報もある (注：根拠は不明)。不足な部分は、適宜 IEC 61508 を参照してアセスメントする必要がある。また、油圧回路の分析方法がほとんど書かれておらず、新規追加のコンテンツが必要である。
- ・別の米国専門家意見
電気系・油圧系とも、これまでに開発完了したものにわざわざ時間をかけて MTTFd や DC の計算をしても、製品の安全性が上がるとは思えない。ISO 13849 には油圧システムについての要求事項が殆どないが、それでよいのではないか。下記のことができていれば十分と考える。
 - 1) 故障を検出する
 - 2) オペレータに異常を提示する
 - 3) 車体を (必要に応じ) ディレイトする
- ・私見であるが、機能安全の規格は本来電気電子システムが対象であり、電気電子システム以外をスコープに含めるべきではない。建設機械では、本来ならば EN 474-1 が電気電子制御は ISO 19014 (ISO 13849 でもよい) に適合、油圧システムについてはステアリングは ISO 5010 に適合、ブレーキは ISO 3450 に適合…というように、サブシステムごとに安全要求を決めればよいと考える。(残念ながら、報告者は EN474 の策定に直接関与できないが)
- ・IEC 61508 に Graceful Degradation (システムに故障があった時にクリティカルでない機能から切り捨てていく：IEC 61508-7 (2010) Annex C C.3.8) という記述があるが、建設機械のコントローラではどのように実現できるのか不明。このような記述は、ISO 19014 では除くべき。

〈Part 1〉

- ・車体全体のリスクアセスメントを「ISO 12100 リスクアセスメント」、制御系のリスクアセスメントを MCSSA (Machine Control System Safety Analysis) と名付ける。
- ・Part 5 の膨大さに懸念が示され、ISO 19014 以外のリスクグラフを使ってもよいことにしようという提案がされた。一応、案文には “This part of ISO 19014 provides guidance and a methodology…” となっており “the methodology” ではないので辻褄はあっているのだが、the methodology をつくるのが ISO 19014 の目的だった筈。やはり、リスクグラフは標準化できないのか…。
- ・MCSSA は必須。ただし MCSSA の結果 QM になったものは Safety Related Parts of Control System ではないので、Part 2, Part 3, Part 4, part 6 の要求事項は適用されない。
- ・被害度 S3 で暴露確率の低い (ドラフトでは $E=E0$ かつ $C=C0$) ものについて QM が許されるのかという議論が出たが、建機では tolerable risk と考えることとなった。但し、逆に E だけが E0 または C だけが C0 に対し全て QM というのは認められなかった。(2016 年 5 月の日本での会議において、日本から意見提出したが却下されている。今回イタリアから再度意見提出されたが、再度却下)

〈Part 4〉

- ・Part 4 の NWIP 投票に対し、日本は CD から始めることには反対せず、約 1 ページのコメントを提出しているが、米国は 30 ページのコメントを提出し、WD から開始すべきとの意見。
- ・ソフトウェアツールを買い直したり、ツールの認証のために追加費用を払うことが必須とならないような案文とすべきという意見があった。

〈Part 5〉

- ・アタッチメントは全種類を網羅しなくてもよいのでは。母機メーカーが売っているものは対象だが、アタッチメントメーカーのブランドで売っているものはアタッチメントメーカーが責任をもつべき。ISO 19014 では代表的なもののみ扱う。
- ・ホイールローダの作業機のリスクアセス見直し (MPLr=d → c)
正しい使用においては作業機の下に人はいないはず。
- ・マテリアルハンドリングにおいて、バケットが下げ方向へ誤動作した場合、円柱状の資材 (パイプなど) を抱えていると、落下して人に当る、というシナリオがあったが、そのような物体は本来パレット等に

固縛すべきであり、それを前提にしたアセスメントにすべきということになった。固縛すればパレットに載せているものが落下することはない、ということでオーストラリア PL が E を 1% と書こうとしたが、「可能性がないならリスク自体なしにすべき」と指摘し、受け入れられた。

- ・公道上でのステアリング故障の ($MPLr = e \rightarrow d$) に見直し

但し、 $MPLr = d$ だと公道上のステアリングがカテゴリ 2 でも実現できることになるが、現実的か? という疑問が米国専門家より提示された。(ステアリング機能は車両停止まで機能維持する必要がある、冗長性が必要ではないか)

- ・カメラ, Hazard Detection System

カメラについては、画像のフリーズについて $MPLr = c$ に見合った設計が必要。画像のフリーズ自体で人が死ぬわけではないが、画像を信用した結果、人を轢いてしまう S パラメータが採用されている。制御系（出力が物理的な動きをひきおこすもの）以外を規格のスコープに含めることには反対意見も出ており、拡大解釈にも思えるが、Part 1 に「Immediate Action Warning については ISO 19014 の設計原則を適用する」という文章があるため (Part1 Annex B), 反対する場合は十分な論理構成が必要と思われる。

以上

