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）2016 年 8 月～ 9 月 英国ロースター市 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）内の特設グループ会議が 2016 年 8 月～ 9 月にかけて英国ロースター市で開催され，協会標準部会 ISO/TC 127 土工機械委員会から前回 7 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 国際作業グループ内 Ad Hoc Group（特設グループ）会議

1 開催日：平成 28 年 8 月 29 日（月）～ 9 月 2 日（金）

2 開催地：英国ロースター市 JCB 本社

3 出席者：10 名

米国 Part 2 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
イタリア Part 4 プロジェクトリーダ
オーストラリア Part 5 プロジェクトリーダ
スウェーデン 1 名
日本 1 名

4 会議概要

Part 2（制御システムの実装と評価）

・当初予定になかったが CD 投票の結果コメントが多数出たため，議題に追加された。
・技術（te）コメント以外の審議を行った。（2016 年 11 月末予定の WG 全体会議で技術コメントの審議に集中するため）
・技術コメントに絞っても，上記 11 月末の会議で審議しきれない可能性が高くなった。このため，Part 2 を今後どのように進めるかを 11 月末の会議で決定する。（自発的キャンセルを行って再スタートの可能性が高い。）
・事前にコメントで指摘した通り，「並列加算」の記述に技術的不備がある事が理解された。この部分の修正案文を日本が提案することにした。
・要求される（required）レベルを MPLr，実現できた（achieved）レベルを MPLa とし，単位（尺度？）として用いるときは MPL と使い分けることにする。

Part 4（ソフトウェアへの要求事項）

・日本コメントについて説明を行った。MPLr に応じた書き方となるよう，米国専門家が「バス通信への要求事項」の案文を考える。
「6.2 のバス通信のモデルについては不要」に対して，プロジェクトリーダより「安全メッセージと非安全メッセージを分離することを示すため必要なものがある」と回答された。
・米国専門家より，「SAE J1939 の safety taskforce では J1939 で対応できるのは PL = b まで。PL = d まで対応できるプロトコルはメッセージを 2 個送る」との報告あり。
一方で，別の米国専門家から「CAN（SAE J1939 のことか）を使ったステアリング（PL = c 以上？）が問題なく動いている」という意見も出た。（PL は ISO 13849 での達成レベル。今のところ MPLa = PL）
・手法の非推奨を表す記号は “x” から “-” に変更する。

Part 5（Part 1 の実施例）

・Part 1（リスクアセスメントの方法と MPLr の割り当て）のプロセスを試行してみるという予定だったが，その前にシナリオを検討する際の前提条件（Assumption），Exposure の考え方（大まかに言えば危険に晒される時間比率なのだが，分子と分母がそれぞれ何かという議論），Controllability の決め方についての議論があり，これで時間切れとなった。

5 今後の予定

・2016 年 11 月末 -12 月初め WG 会議 @ 米国フロリダ州ドラル John Deere 社オフィス
Part 1 DIS 投票に対するコメント審議
Part 2 CD 投票に対するコメント審議，DIS 原稿の準備
Part 3（耐環境試験）DIS 投票に対するコメント審議
Part 4 CD 案文の準備
・2017 年 1 月末または月半ば AdHoc 会議 場所未定
Part 5
・2017 年 9 月初め WG 会議 場所未定
Part 2 DIS 投票に対するコメント審議

Part 4 CD 投票に対するコメント審議

・Part 1（要求レベルである MPLr を決める部分）が先行しているため，Part 2（達成したレベル MPLa の評価）とミスマッチになった場合は，Part 1 の 2nd DIS を発行して調整する予定。

6　日本のアクション（今回議題になっていないパートも含めて）

Part 1，Part 5

Part 1 の内容を試行して Part 5 を作成し，その結果を Part 1 にフィードバックすべきと思うが，まず Part 1 を決めてしまい，その後で Part 5 を作ればよい，という考えで進めているように感じられる。いずれにしても MPLr が高すぎるのは問題であり，試行例をできるだけ集めて問題点を指摘すべき（可能なら代案を出すべき）と考える。Part 1 の DIS 投票期限は 2016 年 11 月。

Part 2

電気を使用しない制御システムについてどのように記述すべきか日本案（案文）を WG に提案する。電気電子制御システムについても，ベースとなる ISO 13849 であまり説明されていない部分の記述を決めていく必要がある（詳細な要求をしないならしない，要求するならどういう要求事項にするか）。2016 年 11 月末～ 12 月初めの WG 会議で扱う。

Part 3

ランダム振動試験の試験水準は日本宿題となっており，試験水準についてどの程度にすべきか意見を募集する。

Part 3 には大きな争点はないが，ISO 15998-1 の環境試験の項目を参照している規格は，今後 ISO 19014-3 を参照することになると思われ，注意が必要と考える。（メーカの判断により独自の試験水準を設定できる余地が少なくなっている。）Part 3 の DIS 投票期限は 2016 年 11 月半ば。

Part 4

バス通信が過大な要求にならないようにする。2016 年 11 月末～ 12 月初めの WG 会議で扱う。

7　議事メモ

Part 4（ソフトウェアへの要求事項）

1）Part 4 に限った話ではないが，認証？者の独立性について議論があった。

・3rd party が必須ではない筈。

・独立した社内組織でよい筈。

・機械指令は自己宣言であり，認証機関が必須ではない。

・会議参加者（社）の間でも，全て社内組織，SIL/PL が高い場合のみ認証機関を利用するなど，対応が一様でない。

2）4.3 Software architecture design

MPLr=e に対し informal methods も可とする

ソフトの FMEA，FTA はシステムレベルで実施すべき→システムレベルとする。

3）4.4 Language，library，and tool selection

Tools with increased confidence とは：自分で判断してよい。

ツールを買い替えたり，後追いで認証を取得する必要はない。

4）4.5 Software design and coding

No dynamic variables or objects と Online checking を選択にする。

online checking は IEC 61508 の定義を引用する。

静的に解析してメモリがあふれないことを証明できるなら，それでもよい。

IEC 61508-3 の dynamic variable と dynamic object の違いは何か？

メモリが足りないという問題は一緒ではないか。

stack area は静的に配置されているので，stack は dynamic object ではない，とする。

5）4.6 software module testing

coverage test は IEC 61508-3 から変更し，WG の推奨とする。

MPLr=e はブランチカバレッジ 1 択。

Performance test は integration test で行うほうが自然だが，module で実施したいユーザの為，このままにしておく。

Part 5（Part 1 の実施例）

・Exposure において，例えば，走行中にステアリングが故障したとしても，機械後方には被害が及ばないはずであり，その面積比率を乗じるべきではないか。

・Controllability では，AR（Ability of React）の判定基準として，回避手段の数よりもオペレータの反応の方が重要ではないか（本能的な操作が行われるか否かで判定してはどうか）との意見が出た。DIS に対する英国コメントに織り込まれる予定。

・前提条件（Assumption）について

例えば「自動車のエアバッグはシートベルト装着を前提にしている」という意見が出て，建機においても single point failure（操作ミスと機械の故障は同時に起らない）の前提に立ち，「機械は正しく使われていて，リスクアセス対象でない他の安全装置は正常とする」とされた。

以上