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 3 月ドイツ・カイザースラウテルン市 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 3 月にドイツ国カイザースラウテルン市で開催され，協会標準部会 ISO/TC 127 土工機械委員会から前回 12 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 3 月 15 日（火）～ 18 日（金）

2　開催地：ドイツ カイザースラウテルン市 JohnDeere 社オフィス

3　出席者：11 名

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

4　決定事項

CD 19014 Part 1 については，議論の結果を特設グループのコメントとして提出する。Part 2 ～ 4 については，各担当プロジェクトリーダが作業案文に議論の結果を織り込む。

5　議事メモ

Part 1（リスクアセスメントの方法と MPLr の割り当て）

5.1　リスクグラフの入力となる 3 つのパラメータが個人の主観によってばらつかないように，定義を詳細にする。3 つのパラメータとは「人的被害の大きさ（S：Severity）」，「危険な状況への暴露度合い（E：Exposure）」，「危険な状況を制御して（避けられる）度合い（C：Controllability）」である。

① S：Severity

例えば，道で滑って転んだ場合の Severity として，最悪は頭を打って死亡から，軽い打撲で済む場合までありうる（これの中間として骨折等もある）が，どのレベルを採用すべきか？となると，Severity には確率的分布がある，という議論が行われた。

2015 年 8 月の特設グループ会議で Exposure の閾値に正規分布が持ち出されたのは，危険な状況への曝露確率とこの議論が混同された為であることが判明した。

② E：Exposure

機械の稼働時間のうち，危険な状況に晒されているのは何時間か，という比率を使用することとなった。

③ C：Controllability

Controllability に貢献する要因に分解して決定する方法が踏襲される。C に対する個別のリスクグラフを新たに設けるのに等しく，少々凝りすぎのようにも思われるが……。

リスクアセスにおける運転員以外の登場人物として，Bystander と Coworker の Controllability を分けるべきという意見が出た。Coworker は工事施工の関係者なので安全の教育訓練を受けているが，Bystander には一般の子供・老人も想定されるため。サービスマンの扱いについては，オーストラリアの宿題とされた。

5.2　E：Exposure の尺度やリスクグラフについては，妥当な方向に修正されている。リスクグラフについては，現行規格と大きく乖離しないよう更に Calibration を行う必要があるというコンセンサスはある。（作業は未実施）

Part 2

・CPU は well-tried component（枯れた技術とでもいうのだろうか）と言えるかどうか，現実のコントローラのカテゴリは何か，という議論が行われた。
―CPU は複雑なので，well-tried component とは言えないのではないか。この記述は ISO 13849 にあり，ISO 19014 の案文を作成するときに意図的に削除したのだが，復活する。

―但し，現実のコントローラはCPUを単体で使っているわけではなく，いろいろな診断回路（ウォッチドッグタイマ等）を持っているので（カテゴリ2にどの程度の要求をするかにもよるが）仮にカテゴリ2と言えないとしても，カテゴリ1（或いはB）より上の筈である。（カテゴリ1やBには診断機構は全くないので）

・油圧ステアリングの問題

公道走行する土工機械のステアリングシステムには，高いMPLr（dやe）が割り当てられる可能性が高いが，一方で，これまで実績のある油圧ステアリングはカテゴリ2や3の要件を満たす二重系でもなく，診断回路も設置されていない。

ISO 13849に従えば，公道走行する土工機械（かつ車速の高いもの）でオービットロールなどは許容されないこととなり，現実に合わない。オーストラリアの専門家が様々な対応案を説明したが，皆を納得させることはできなかった。

Part 3（耐環境性要求）

今回はPart 3については作業なし。2016年5月に東京で予定される会議でCDコメントについての審議を行う。

Part 4（ソフトとバス通信に対する要求事項）

・ソフトウェアに特化した内容の為，参加人数が減少した。

・雑談で車両ハッキング（cybersecurity）の話題が出る：SAEからペーパーが出ているらしい。（SAE J3061作成中）ホットな話題であるが，ISO 19014では扱わないこととする。

・Table 1（Software safety requirement specification フェーズで使用する手法）

computer aided specification toolはSIL3（MPL=e）から要求。

semi-formal methodsとはgraphical representationのこと。

formal methodはまだ使えるレベルにないのでは。（他のフェーズでも）

inspectionとwalk throughの違い：inspectionは設計者以外の者がチェックする。

inspectionはIEC 61508ではSIL3から，農機ではSRL2から要求されている。

19014 Part 4の案文では，MPLr=dからinspection要求となっている。

・案文の内容以外に関する議題（余談）

・今回の会合に先立って日本はPart 1，Part 3の投票及びコメント送付を行っているが，3月下旬の投票締切まで投票内容はコンビナーに通知されない為，投票内容を反映せずに議論が行われた。

・ドイツがISO 19014に全面反対（ISO 13849そのまま使用を要求）の為，欧州のメンバー内では妥協点を探る活動をしている模様。例えばドイツは，ISO 19014 Part 1のドラフトのリスクグラフにQM（機能安全上の要求なし）が目立つのに難色を示しているらしいので，今回会議で提示された案文では，E0，E1を無くしてQMを目立たなくしている。

以下参考

会議時点での最新案文N 108（CD投票に添付）と，今回会議で合意したAdhocグループ案の比較。

● Exposure - Table 2（N 108）（**表―1**）

● Exposure - 特設グループの修正案（**表―2**）

・頻度ではなく時間比率とする。（CDに対する日本意見と一致）

・そのうえで，1%未満は層別しない。（日本意見と異なる）

・頻度の記載は削除された。（日本意見には残すようにしてあるが，無くてもよい）

● Controllability - Table 3（N 108）（**表―3**）

● Controllability - 特設グループの修正案（**表―4**）

・C2の閾値は90%とする。（意見提出はしていないが，

表―1　Exposure - Table 2（N 108）

E0		E1	E2	E3	E4
Very low possibility (theoretically possible; once during lifetime)		Rarely (more than once per year)	Sometimes (more than once per month)	Often (once or more a day)	Frequently (almost every operation)

表―2　Exposure - 特設グループの修正案

E2	E3	E4
＜%	＞1 to ＜0%	＞10%

表―３ Controllability

ISO 19014-1:2015(CD)

C0	C1	C2	C3
Easily controllable The operator or bystander controls the situation, and harm is avoided.	Simply controllable More than 99% of people control the situation.	Mostly controllable More than 50% of people control the situation.	None The average operator or bystander cannot generally avoid the harm.

表―４ Controllability - 特設グループの修正案

C0	C1	C2	C3
Easily controllable The operator or bystander controls the situation, and harm is avoided.	More than 99% of people control the situation. In more than 99% of the occurrences, the situation does not result in harm.	More than 90% of people control the situation. In more than 90% of the occurrences, the situation does not result in harm.	None The average operator or bystander cannot generally avoid the harm.

表―５ Controllability の決め方 - 特設グループ案

No of alternative actions / controls to mitigate failure	Awareness level of failure	Ability to react	Admin controls / site management
Yes (1)	High (3)	Good (3)	Always good, enforced by law (1) or not relevant
	Some (2)	Some ability (2)	relevant but Sometimes good / some enforcement (0.5)
	Low (1)	Low (1)	
No (0)	None (0)	Very low (0)	

Category	Score - when admin controls are relevant
C0	9
C1	6
C2	4.5
C3	＜4.5

農機規格ISO 25119と同じ90%とするのが好ましい。）

● Controllability の決め方 - 特設グループ案（**表―５**）

Definitions required for awareness, ability to react, alternative actions / controls and admin controls

●リスクグラフ - Figure1（N 108）（**表―６**）

●リスクグラフ― 特設グループの修正案（**表―７**）

・CD 案文より MPLr が１段階下がった。（農機規格 ISO 25119 と同レベルになった）

・E1 以下が削除された。

・C0に対してもMPLrにaやbが割り当てられている。（日本意見は「C0 はオペや周囲の人が容易に危険を避けられるという定義であり，建機の使われ方としてはリスクなしとすべき」との考えから，C0 に対しては QM を提案）

表―6　リスクグラフ - Figure1（N 108）

		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	a	b	c	d
S2	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	a	b	c	d
	E4	b	c	d	e
S3	E0	QM	QM	a	b
	E1	QM	a	b	c
	E2	a	b	c	d
	E3	b	c	d	e
	E4	c	d	e	e

Key

S = severity

E = exposure to hazardous event

C = controllability

QM = quality measures

a, b, c, d, e = required Machine Performance Level MPLr

表―7 リスクグラフ― 特設グループの修正案

		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	a	b	c	d
S3	E2	QM	a	b	c
	E3	a	b	c	d
	E4	b	c	d	e