部 会 報 告

ISO/TC 127/SC 2/WG 22 (ISO 17757 土工機械及び鉱山—自律式機械・鉱山システム安全) 2016年5月カナダ・バンクーバー市 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) 遠嶋 雅徳 (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 22 (ISO 17757 土工機械及び鉱山—自律式・半自律式機械及び鉱山システム安全) 作業グループ会議が 2016年5月にカナダ国バンクーバー市で開催され、前回 2016年3月に続き協会標準部会 ISO/TC 127 土工機械委員会から国際専門家 (Expert) として出席した遠嶋雅徳氏の報告を紹介する。

1 開催日：2016年5月5日 (木)～6日 (金)

2 開催地：カナダ国バンクーバー市

Wenco International Mining Systems 社
会議室

3 出席者：11名

米国 (ANSI) プロジェクトリーダー, 他4名

カナダ (CSA) 4名

日本 (JISC) 2名

4 会議結果概要：

DIS ドラフト作成に向けて、最新の CD (Committee Draft) のレビューを実施した。最新 CD は4月に配布されたが、それに対してコメントを提出したのはカナダと日本のみであった。実際、今回の WG 会議に出席したのは議長を除いて10名のみ (米国・カナダ・日本) であり、会議が始まる前には、既に作業が終わりに近づいている雰囲気すらあった。

しかし、WG 会議では相変わらず細かい議論となり、大きく内容が変更されることはなかったものの、文書の構成や表現、用語の定義等に大幅な修正が行われた。

日本からは、ステアリング異常時の “shall maintain safe state” という要求は現実的でなく、“bring to safe state” が妥当というコメントを出していたが、受け入れられなかった。

本規格では、“safe state” = Risk Assessment で決まる acceptance level 以下の安全状態であること、と定義している。例えばステアリング故障で走路を逸脱しても、それによる被害が要求安全レベルより小さいならば safe state であるというのが WG 全体での認識

である。つまり、機能安全的な発想で考えるべき、ということで、これは本規格全体に共通するコンセプトである。

なお、本プロジェクトは本来であれば2016年内に終了予定であったが、日程的に難しい為、9ヶ月の延長が提案され承認されている。とにかく期限内に本規格を発行した後、次の Phase 2 で更に細かい内容を追加していこう、というのが米国プロジェクトリーダーの考えである。

【以下、会議での主な議論】

Barrier system

もともと、地下鉱山で用いられる Sandvik 社の半自律式ロードホウルダンプのコンセプトであるが、これに対するコメントが多数出され、これまで Site Access と呼んでいたものも含めて Aoz Access と呼ぶこととなった。なお、Barrier System も Access Control System と改められた。

また、Barrier system の状態をモニターしなければならぬという指摘があった。通常、鉱山等においては、ゲート等の管理は、システム提供者側でなく使用者側が現場特有のシステムとして実施しているが、リスクアセスメント上必要と判断された場合、それらもシステムとして管理されなければならない。具体的には、Light barrier, Laser beam, Video imaging, RFID などを利用したゲートと規定された。

アクセスシステムに対しての breach (ルール無視) が発生した場合、システムは safe state になり、かつ中央管制システムに notify されなければならない、という議論。breach が発生したら必ず safe state にする事が可能か議論され、D5 Barrier placement でカバーされているので規定できるという結論となった。notify までは必要ないという議論が占めたが、そこまで言うのであれば、という事で最終的に了承され、意見が通った形。

Block Diagram

ブロックダイアグラム自体は、あくまで ASAMS

を実現する場合の例であること、また、ブロックダイアグラムに登場する要素は、本文で記述されるべきと指摘された。

ASAM Supervisor System

もともと Site Supervision System だったが、ASAM (Autonomous and Semi-Autonomous machines) のみが対象という事で Site から ASAM へ変更された。本文に列記されているサブシステム名も他との一貫性がないが、ブロックダイアグラムと同様、一つの例という事となっている。また、GNSS Grand Station と通信関係は必ずしも Supervisor に関係しない、という事で削除された。

Permissions and Security

これまでは Access のみモニターする、となっていたが、exit (egress) についてもモニターする。また、これまでは機械のみがモニターの対象であったが、人も対象に追加された。モニターに加え、エスコートされてもよいとしているので、例えばピックアップトラックに複数の人が乗っていても問題がないと考えられる。

なお、地下鉱山では

- ・トンネル毎に人の入退出を確認する。
- ・5分以上人の動きがない場合、人が倒れているとして扱う。

という管理が実施されているとのこと。

また、モニター又はエスコートされる機器・人に対して、位置、距離、速度、方向、精度等を Risk assessment に応じて明確にしなければならない、という記述が追加された。

Steering System

ステアリングの Single electric failure 時にも “maintain safety state” しなければならないという記述の件で日本から “maintain safety state” は現実的でなく “bring to safety state” としたらどうかと提案したが通らず。“safe state” とは絶対的な安全ではなく、acceptable risk 以下の安全状態と定義されるので、故障する確率や、その時に周囲に有人車両がいる確率等を考慮して対応されるべきという議論となった。

用語の定義

この期に及んで autonomous/semi-autonomous の議論が再燃し、変更が実施された。

Autonomous mode/Semi-Autonomous mode/Autonomous Machine

もともと Autonomous machine が先に定義され、Autonomous machine として機能している時が Autonomous mode となっていたが、その定義順序が逆となった (autonomous mode で動作する機械を autonomous machine と呼ぶ)。これが最後の議論になることを祈る。

Mode indicator

“hold mode” と “hold state” の違いが明確でないとの意見が米国から提出され、モードランプから “hold” の部分が削除された。

Mode

unexpected (予期しない) 又は unauthorized (権限のない) モード変更が実施されることで、安全を脅かしてはならない、と議論された。

Communication & Network

Design する際には industry standard を参照するという要件が追加された。

また、リモートアクセスによる spoofing (なりすまし) 等にも対応しなければならない、と議論された。例えば、data encryption や password 等で対応するのが通常だが、password のみでは不十分という意見もあり、user authentication (ユーザ認証) という表現に改められた。

西オーストラリア州の自律機械の実施要領

特に Operation 関連の項目で、既に西オーストラリア州で発行されている “CODE OF PRACTICE Safe mobile autonomous mining in Western Australia” がそのまま引用されているが、最新版との整合性を確認し、shall/should の表現統一を実施した。Informative の Annex からは全ての “shall” が削除された。

文書の構造

現在のドラフトの構成に統一感がなく、分類も正確でない (onboard かどうか等) という指摘があり、一から書き直すべきとの意見も出された。現時点で CD からやり直すと、最低でも 2 年かかってしまうので、さすがにそれは却下され、最低限の構成変更を実施することとした。

以上