厚生労働科学研究費補助金（労働安全衛生研究事業）
総括研究報告書

自動制御システム等による車両系建設機械と協働する場合に新たに生じる労働安全衛生リスクのシステム思考に基づく分析フレーム

研究代表者　澁谷　忠弘　横浜国立大学　総合学術高等研究院　教授

研究要旨
近年、産業用ロボット等の多様な機械システムにおける遠隔化・自動化・自律化による労働災害の防止・軽減効果が期待されている。しかし、制御システムに代表される高度な技術の新規導入は、労働災害リスクを低減すると同時に、別の新たなリスクを生み出す可能性がある。したがって、これら制御システムの新規導入を想定した適切なリスクアセスメント（RA）を実施する必要がある。機械安全分野において用いられてきた従来手法は、対象となる機械システムを構成する個々の要素の故障に起因した事象の分析に対しては有効な手法である一方で、個々の要素間の相互作用が多数存在する自動化・自律化された機械システムの分析は困難である。そこで本研究は、自動制御システム等による車両系建設機械と協働する場合に新たに生じる労働安全衛生リスクを分析するためのフレームを構築することを目的とする。システムの構成要素間の相互作用に起因する事象を記述する、システム思考に基づくモデル（STAMP）に着目し、STAMP/STPAを用いてハザード分析を行うとともに、車両系建設機械と協働する労働者の作業HAZOPを実施し、これらの結果を組み合わせることで、協働において懸念されるリスクを体系的に抽出する。抽出されたリスクに対してモデルベースアプローチによる定量評価を取り入れることで、リスク分析の高度化を目指し、最終的には、労働災害被災リスク、リスクの評価手法、リスク評価に基づく労働災害防止対策について必要な項目を整理する。

A. 研究目的

本研究は、自動制御システム等による車両系建設機械と協働する場合に新たに生じる労働安全衛生リスクを分析するためのフレームを構築することを目的とする。STAMPモデルを用いてハザード分析を行うとともに、労働者の作業HAZOPと組み合わせることで労働者との協働において懸念されるリスクを網羅的に抽出することを目指す。また、STAMP/STPAやHAZOPではガイドワードを用いたリスク特定であるため、2年度目にはモデルベースアプローチによる定量評価を取り入れてリスク分析手法の高度化を目指す。最終的に、労働災害被災リスク、リスクの評価方法、リスク評価に基づく労働災害防止対策について、これまでの建設機械の労働災害防止マニュアルの差分として必要な項目を整理する。

B. 本研究の背景・目的および研究の全体像

近年、産業用ロボット等の多様な機械システムにおける遠隔化・自動化・自律化が積極的に進められている。これら技術開発は、適切な制御システムを用いて制御されることにより、従来労働者が担ってきた様々な作業を労働者に代わって実行することができるため、労働災害の防止・軽減効果が期待されている。しかし、制御システムに代表される高度な技術の新規導入は、労働災害リスクを低減すると同時に、別の新たなリスクを生み出す可能性がある。したがって、これら制御システムの新規導入を想定した適切なリスクアセスメント（RA）を実施することで、上述の新たなリスクを含む一連のシステムのリスクを把握し、許容可能であるかどうかを確認する必要がある。

機械安全分野におけるRA手法としてはこれまで、Failure Mode and Effects Analysis（FMEA）やFault Tree Analysis（FTA）などのシステム工学的な手法が用いられてきた。これらの手法は、対象となる機械システムを構成する個々の要素の故障に起因した事象の分析に対しては有効な手法である。しかし、自動化・自律化された機械システムは個々の要素間の相互作用が多数存在する複雑システムであり、従来手法はこれら相互作用に起因した事象を分析することが困難であった。一方で、近年ではシステムの構成要素間の相互作用に起因する事象を記述する、システム思考に基づくモデル等も提案され、制御システムなどにおいて生じる構成要素間の連携不具合に起因した事象を考慮した上での分析も可能となってきている。特に、代表的なモデルであるSystems-Theoretic Accident Mode and Process（STAMP）モデル[1]に基づいて制御構造をモデル化しシステムレベルでのハザード要因を分析する安全解析手法STPA（STAMP based Process Analysis）[2]は、車両分野の機能安全国際標準規格ISO26262[3]の最新版において安全解析手法の一つとして採用されるなど、自動運転分野において注目されている。

本研究は、自動制御システム等による車両系建設機械と協働する場合に新たに生じる労働安全衛生リスクを分析するためのフレームを構築することを目的とする。本研究の全体像を図1に示す。車両系建設機械における自動制御システム等によってもたらされるリスクは、従来の信頼性工学の視点に基づくFMEAやFTA等の技法では抽出が困難である。そこで、まず初年度においてSTPAを用いてハザード分析を行うとともに、車両系建設機械と協働する労働者の存在を想定したHAZOPおよび作業HAZOPを実施し、これらの結果を組み合わせることで、協働において懸念されるリスクを体系的に抽出することを目指す。HAZOP、作業HAZOP、およびSTPAの実施にあたっては、建設荷役車両安全技術協会や日本クレーン協会、建設機械施工の自動化・自律化協議会に所属する専門家等との協力連携および意見交換しながら検討を進めた。

上記手法ではガイドワードを用いた分析が行われるため、その結果は定性的なものにならざるを得ない。そこで、次年度においては抽出されたリス

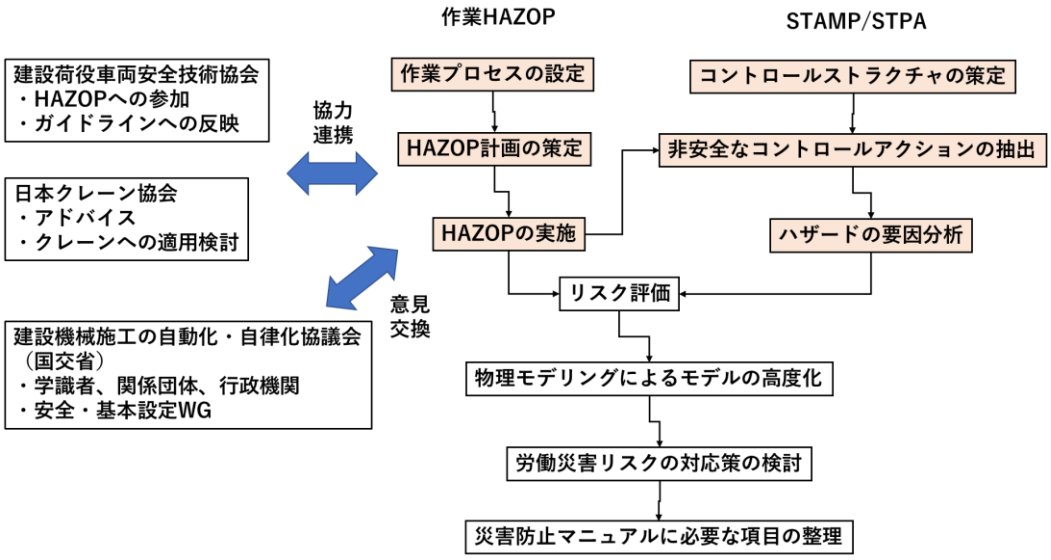

図 1　本研究の全体像

クに対してモデルベースアプローチによる定量評価を取り入れることで、リスク分析の高度化を目指す。最終的には、労働災害被災リスク、リスクの評価手法、リスク評価に基づく労働災害防止対策について、これまでの建設機械の労働災害防止マニュアルの差分として必要な項目を整理する。

本報告では、自動運転する車両系建設機械と労働者の協働において生じるリスクシナリオ特定を目的として実施した、HAZOP、作業HAZOPおよびSTPAの結果について述べると共に、次年度検討における課題および実施項目を整理した。

C. HAZOPを用いたリスクシナリオ抽出

HAZOPとは、正常状態あるいは設計上意図されたシステムの状態から、何らかの原因により生じた逸脱に着目し、その結果を専門家集団によるブレインストーミング式に想定することでリスクシナリオを特定する手法である[4]。ここでは、仮想の建設現場に存在する自動運転の油圧ショベルによる掘削・放土作業を対象とし、当該ショベルの可動域付近に作業者が存在することを想定した分析を行った。想定作業における油圧ショベルの動作手順は以下の通りとした。

(1) 目標地点への移動(および旋回)
(2) (アーム駆動および)掘削
(3) (バケットの)引き上げ
(4) 旋回
(5) (バケットからの)放土

使用するガイドワードとしては、油圧ショベルの自動運転を想定し、文献[4]を参考に、センサー情報等を対象としたソフトウェアver.（表1）と、ハードシステム等を対象としたハードウェアver.（表2）の2種類を用意した。実施した結果の一部を表3に示す。各作業手順に対して用意したガイドワードをそれぞれ適用し、その逸脱に物理的意味があるかどうかを判定した上で、逸脱の原因と結果を想定した。ソフトウェアに関しては、自動運転制御に必要となるショベルの移動信号および停止信号、周辺状況把握のためのセンサーデータの不備により、油圧ショベルの意図しない挙動が引き起こされ、周辺作業者に接触するシナリオ等が特定された。ハードウェアに関しては、油圧ショベルの物理的故障等により、油圧ショベルの意図しない挙動が引き起こされ、周辺作業者に接触するシナリオ等が特定された。

表 1　HAZOP ガイドワード ソフトウェア ver.

ガイドワード（ソフトウェアver.）		
逸脱の種類	ガイドワード	解釈の例
否定	NO	データまたは制御信号なし
定量的修正	MORE	データが想定より高速で通過する
	LESS	データが想定より低速で通過する
定性的修正	AS WELL AS	ある余分の信号または不要な信号があある
	PART OF	データまたは制御信号が不完全
置換	REVERSE	通常では関連性がない
	OTHER THAN	データまたは制御信号の誤り
時間	EARLY	規定時刻を基準にして信号の到着が早すぎる
	LATE	規定時刻を基準にして信号の到着が遅すぎる
順序またはシーケンス	BEFORE	シーケンスの中で信号の到着が予定より早い
	AFTER	シーケンスの中で信号の到着が予定より遅い

表 2　HAZOP ガイドワード ハードウェア ver.

ガイドワード（ハードウェアver.）					
適用区分		日本語ガイドワード			
動作の量	動作の有無	全く～しない			
	力の程度	強く（力強く）	弱く（弱々しく）		
	動作速度	急いで	ゆっくり		
	持続時間	ずっと（連続して）	ちょっと（一時的に）		
	動作範囲	余分に	不十分に		
動作の向き	方向	反対に	他の方に		
	回転	反対に（逆に）			
動作の種類		違う～する			
動作の対象	対象物	違うものに			
	被対象物の向き	反対に（逆に）			
	被対象物の量	多く	少なく		
時間		前に	後に	同時に	別々に
順序		繰り返して	反対に（逆に）		
回数		多く	少なく		

D. 作業HAZOPを用いたリスクシナリオ抽出

STAMP/STPAモデルを用いた車両系建設機械のハザード分析を行うための事前解析として、自動制御システムを用いた車両系建設機械において懸念される事故シナリオを抽出する作業HAZOPを実施した。作業HAZOPの実施にあたっては、自動制御システムを用いた車両系建設機械における作業フローを定義する必要がある。そこで、令和2年3月に国土交通省から発行された、「自動追尾トータルステーション（TS）・衛星測位システム（GNSS）を用いた盛土の締固め管理要領」[5]を参考とした。これは、「河川土工及び道路土工等において、TS又はGNSSを用いた盛土の締固め管理に適用する」という記載があり、本研究の自動制御を用いた車両系建設機械に関する作業に該当すると考えた。この要領では、図2のように自動制御システムのための作業フローが記載されている。図中の赤字が自動制御のために新たに必要になった作業である。図3、図4はそれぞれTSを用いた場合、GNSSを用いた場合の作業の内容である。

上記作業内容を基にずれを以下のように設定した。これらのずれでは自動制御システムを使用する上での作業(確認・認識)行為が達成できない、不十分である状態を表現している。これらのずれと図2～図4の作業内容により自動制御システムを用いた車両系建設機械のシナリオを抽出した。

・悪意のある設定
・確認・認識行為ができない
・確認・認識すべきデータがない、取得できない
・確認・認識すべきデータが多い、少ない
・確認・認識すべき行為やデータ表示、データ取得タイミングが早い、遅い
・確認・認識すべきデータやものが大きい、小さい
・確認・認識すべきデータの精度が悪い

実施した結果を表4に示す。特徴的なものは、テロ行為などの悪意のある設定、自然災害や太陽フレアの発生による通信障害による事故シナリオと自動制御での車両系建設機械に関する作業行為の未達成及び不十分行為による事故シナリオが認識された。

E. STAMP/STPAを用いた制御システムのハザード分析

近年の機械システムの発展および高度化により、システムを構成する構成要素が増大したこと、また、その構成要素間の関係性が複雑化していることなどの要因により、安全上の課題としてその事故の原因が変容している。Levesonは、このような高度化したシステムの事故の原因として、従来のアクシデントモデルとは異なる、新たなアクシデントモデルを提唱した[1]。それは、「システム理論に基づくアクシデントモデル」であり、STAMP(Systems Theoretic Accident Model and Processes)と命名されている。このモデルは、制御系（コントローラー）と被制御系（被コントロールプロセス）を含む一連の制御システムを想定したとき、仮にその両者が共に正常に動作していたとしても起こり得る事故について言及したものである。その原因は、「認識の不整合」と呼ばれる。すなわち、コントローラーが想定する被コントロールプロセスの状態が、実際の被コントロールプロセスの状態を正しく反映できていないことを意味している。これにより、コントローラーが被コントロールプロセスに対して不適切な制御指示を与えることになる。こうしたアクシデントモデルSTAMPを前提として「アクシデントにつながるハザード」と「その詳細要因」を分析する手法がSTPA(System-Theoretic Process Analysis)と呼ばれる手法である。STPAは、対象とする制御システムモデルに対して、不適切な制御指示が加えられる様々な状況を想定することによって、システムからアクシデントが生じる可能性が潜在している状態（ハザード）や、最終的に発現するシステムの事故（アクシデント）を特定していく手法である。STPAの実施手順を図5に示す。本項では図5の手順に沿って、STPAを用いたハザード分析の実施結果について述べる。

表 3　HAZOP 実施結果（一部）

No.	属性	ガイドワード				逸脱	考えられる原因	結果	既存の管理策	必要な措置
1-S-1	①目標地点への移動	ソフトウェア	NO			信号なし	・ソフトウェアの故障 ・GPSの故障 ・センサーの故障	ショベルが移動しない	・始業前点検	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-2	①目標地点への移動	ソフトウェア	MORE			目標より長い距離を設定	・設定ミス ・ソフトウェアのバグ ・GPS・センサー信号の異常	ショベルが目標よりも先まで進んでしまい、その先で作業している作業者に接触してしまう	・監視員が非常停止する	・入力値の見直し ・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-3	①目標地点への移動	ソフトウェア	LESS			目標より短い距離を設定	・設定ミス ・ソフトウェアのバグ ・GPS・センサー信号の異常	ショベルが目標よりも手前で停止してしまう	なし	・入力値の見直し ・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-4	①目標地点への移動	ソフトウェア	AS WELL AS			センサーから間違った情報の取得	・GPS・センサー信号の異常	ショベルが意図しない方向に移動し、目標に到達せず周辺作業者に接触する	・監視員が非常停止する	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-5	①目標地点への移動	ソフトウェア	PART OF			移動に必要な信号の不足	・設定ミス ・ソフトウェアの故障 ・GPSの故障 ・センサーの故障	ショベルが移動しない	なし	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-6	①目標地点への移動	ソフトウェア	REVERSE			センサの情報の認識間違い	・ソフトウェアの故障 ・GPSの故障 ・センサーの故障	本来するはずのない旋回をしてしまい、周辺の作業者に接触する	・監視員が非常停止する	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-7	①目標地点への移動	ソフトウェア	OTHER THAN			誤信号の送信	・ソフトウェアのバグ ・GPS・センサー信号の異常	ショベルが後退してしまったりアームが旋回してしまったりして周辺作業者に接触してしまう	・監視員が非常停止する	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-8	①目標地点への移動	ソフトウェア	EARLY			移動信号が早く送信される	・GPS・センサー信号の異常	意図しない移動開始で作業者と接触する	・監視員が非常停止する	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-9	①目標地点への移動	ソフトウェア	LATE			停止信号が遅れて送信される	・通信の遅延	適切の停止できず作業者と接触する	・監視員が非常停止する	・センサーの修理 ・ソフトウェアの修理 ・GPSの修理
1-S-10	①目標地点への移動	ソフトウェア	BEFORE			移動信号が予定より早く到着する		ショベルが意図よりも早く移動開始し、作業者がショベルから離れる前に接触する		
1-S-11	①目標地点への移動	ソフトウェア	BEFORE			停止信号が予定より早く到着する		ショベルが意図よりも早く停止し、目標地点に到達しない（保安上の問題は少ない）		
1-S-12	①目標地点への移動	ソフトウェア	AFTER			移動信号が予定より遅く到着する		ショベルが意図よりも遅く移動開始し、目標地点への移動が遅れる（保安上の問題は少ない）		
1-S-13	①目標地点への移動	ソフトウェア	AFTER			停止信号が予定より遅く到着する		ショベルが意図よりも遅く停止し、停止が間に合わず、ショベルが作業者に接触する		
1-H-1	①目標地点への移動	ハードウェア	動作の量	動作の有無	全く～しない	ショベルが動かない	・ショベルの故障 ・信号の受容器の故障	ショベルが目標に到着しない		・日々の動作確認 ・ショベルの修理 ・受容器の修理
1-H-2	①目標地点への移動	ハードウェア	動作の量	動作速度	急いで	ショベルの移動速度が速くなる	・速度制限装置の故障	目標の到着時間が早くなる	・自動停止システム起動	・ショベルの修理
1-H-3	①目標地点への移動	ハードウェア	動作の量	動作速度	ゆっくり	ショベルの移動速度が遅くなる	・モーターの故障	目標の到着時間が遅くなる		・ショベルの修理
1-H-4	①目標地点への移動	ハードウェア	動作の量	持続時間	ずっと（連続して）	ショベルが移動し続ける	・ブレーキの故障	ショベルが暴走し作業者に接触してしまう、目標に到着しない	・自動停止システム起動	・ショベルの修理
1-H-5	①目標地点への移動	ハードウェア	動作の量	持続時間	ちょっと（一時的に）	ショベルが少し移動する	・電子制御装置の故障	ショベルが一定距離移動後停止する、目標に到着しない		・ショベルの修理
1-H-6	①目標地点への移動	ハードウェア	動作の向き	方向	反対に	ショベルの進行方向が逆になる	・駆動装置の故障	目標と反対方向に進む、背後で作業している人に接触する	・自動停止システム起動	・ショベルの修理
1-H-7	①目標地点への移動	ハードウェア	動作の向き	方向	他の方に	ショベルが意図しない方向に進む	・クローラーの故障	意図しない方向に進む、周辺の作業者に接触する	・自動停止システム起動	・ショベルの修理 ・クローラーの修理
1-H-8	①目標地点への移動	ハードウェア	動作の向き	回転	反対に（逆に）	ショベルが意図しない方向に進む	・クローラーの故障(片側のみ)	ショベルが大きく円を描くようにして動くことで周辺の作業者に接触してしまう	・自動停止システム起動	・ショベルの修理 ・クローラーの修理
1-H-9	①目標地点への移動	ハードウェア	動作の種類		違う～する	移動中にショベルが旋回する	・旋回ブレーキの故障	アームが旋回することを想定していない作業者に接触してしまう	・自動停止システム起動	・ショベルの修理
1-H-10	①目標地点への移動	ハードウェア	動作の対象	対象物	違うものに	違う目標に向かって進んでいってしまう	・クローラーの故障(片側のみ)	目標に到着しない、予想だにしない方向に進む	・自動停止システム起動	・ショベルの修理

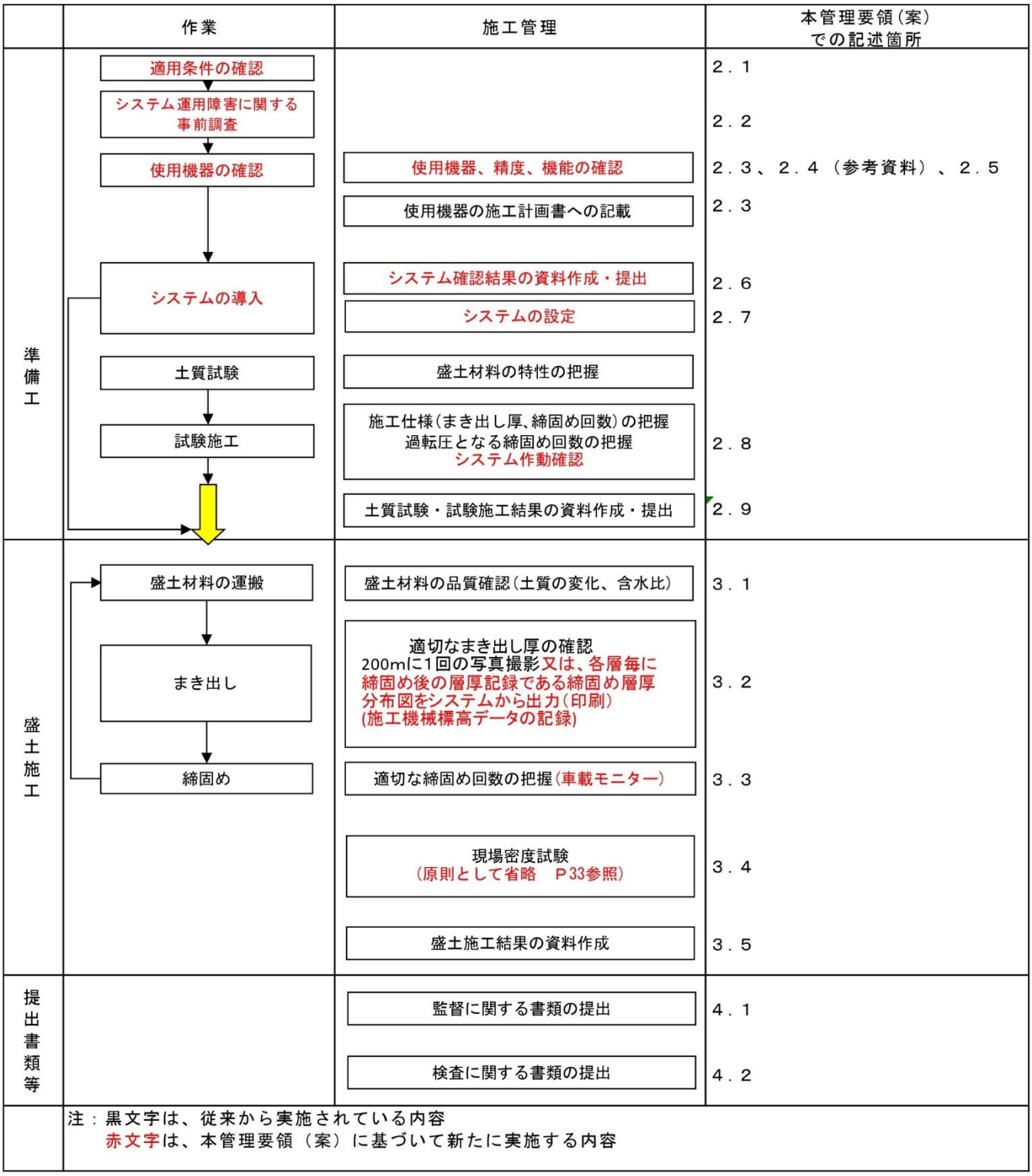

図 2　「TS・GNSS を用いた盛土の締固め管理要領」による
盛土施工の作業及び施工管理のフロー[5]

事前確認チェックシート（ＴＳの場合）

令和　　年　　月　　日

工　事　名：

受注会社名：

作成者：　　印

確認項目	確　認　内　容	確認結果
適用条件の確認	・使用する締固め機械が適用機種(ブルドーザ、タイヤローラ、振動ローラ及びそれらに準ずる機械)であり規格・締固め性能を把握したか？ ・使用する材料が締固め回数管理に適しているか？	
システム運用障害に関する事前調査	・無線通信障害の発生の可能性はないか？ →低い位置に高圧線等の架線がないか、基地、空港等が近くにないか ・ＴＳの視準が遮るような障害物等がないか？	
精度の確認	・ＴＳ測量機器が以下の性能を満足していることを確認できる機器メーカ等が発行する書類（証明書･カタログ・性能仕様書等）があるか？ 公称測定精度　±(5mm＋5ppm×D)　　最小目盛値　20″以下 ・既知座標（工事基準点）とＴＳの計測座標が合致しているか？	
機能の確認	①締固め判定・表示機能 ・ローラまたは履帯が管理ブロック上を通過する毎に、当該管理ブロックが１回締固められたと判定し、車載モニタに表示されるか？ ・管理ブロック毎の累積の締固め回数が、車載モニタに表示されるか？ ・施工とほぼ同時に締固め回数分布図を画面表示できるか？	
	②施工範囲の分割機能 ・施工範囲を、所定のサイズの管理ブロックに分割できるか？	
	③締固め幅設定機能 ・締固め幅を、使用する重機のローラまたは履帯幅に応じて任意に設定できるか？	
	④オフセット機能 ・締固め機械の位置座標取得箇所と実際の締固め位置との関係をオフセットできるか？	
	⑤システムの起動とデータ取得機能 ・データの取得・非取得を施工中適宜切り替えることができるか？ ・振動ローラの場合は、有振時のみの位置座標を取得するようになっているか？	
	⑥締固め層厚分布図作成機能 ・締固め層厚分布図が作成できるか？ ※上記によりまき出し厚管理時の写真撮影を省略する場合は確認する	

図３　「TS・GNSS を用いた盛土の締固め管理要領」に記載されている
TS を用いた場合の作業のチェックシート[5]

事前確認チェックシート（ＧＮＳＳの場合）

令和　　年　　月　　日

工　事　名：

受注会社名：

作成者：　　印

確認項目	確　認　内　容	確認結果
適用条件の確認	・使用する締固め機械が適用機種(ブルドーザ、タイヤローラ、振動ローラ及びそれらに準ずる機械)であり規格・締固め性能を把握したか？ ・使用する材料が締固め回数管理に適しているか？	
システム運用障害に関する事前調査	・無線通信障害の発生の可能性はないか？ →低い位置に高圧線等の架線がないか、基地・空港等が近くにないか ・ＧＮＳＳの測位状態に問題はないか？ →ＦＩＸ解となるのに必要な衛星捕捉数（５個以上）は確保できる状況か	
精度の確認	・ＧＮＳＳ測量機器が以下の性能を満足していることを確認できる機器メーカ等が発行する書類（証明書･カタログ・性能仕様書等）があるか？ 水平（ｘｙ）±20mm　　垂直(z)　　±30mm ・既知座標（工事基準点）とＧＮＳＳの計測座標が合致しているか？	
機能の確認	①締固め判定・表示機能 ・ローラまたは履帯が管理ブロック上を通過する毎に、当該管理ブロックが１回締固められたと判定し、車載モニタに表示されるか？ ・管理ブロック毎の累積の締固め回数が、車載モニタに表示されるか？ ・施工とほぼ同時に締固め回数分布図を画面表示できるか？	
	②施工範囲の分割機能 ・施工範囲を、所定のサイズの管理ブロックに分割できるか？	
	③締固め幅設定機能 ・締固め幅を、使用する重機のローラまたは履帯幅に応じて任意に設定できるか？	
	④オフセット機能 ・締固め機械の位置座標取得箇所と実際の締固め位置との関係をオフセットできるか？	
	⑤システムの起動とデータ取得機能 ・データの取得・非取得を施工中適宜切り替えることができるか？ ・振動ローラの場合は、有振時のみの位置座標を取得するようになっているか？	
	⑥座標取得データの選択機能 ・ＦＩＸ解でのデータのみを取得する機能を有しているか？	
	⑦締固め層厚分布図作成機能 ・締固め層厚分布図が作成できるか？ ※上記によりまき出し厚管理時の写真撮影を省略する場合は確認する	

図 4　「TS・GNSS を用いた盛土の締固め管理要領」に記載されている GNSS を用いた場合の作業のチェックシート[5]

表 4　作業 HAZOP 実施結果

作業	確認事項	ずれ	シナリオ	予想される影響
テロ		悪意のある設定	テロにより悪意のある設定で建機が乗っ取られる。コントロール不能	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
(自然災害、停電、通信量の急増加、システム障害などによる)通信障害		通信できない		建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
適用機種の性能把握	使用する締固め機械が適用機種(ブルドーザ、タイヤローラ、振動ロー ラ及びそれらに準ずる機械)であり規格・締固め性能を把握	不十分	締固め回数にずれが生じる。定期点検、日常点検が正しく行われず故障の原因となる。	転落事故、巻き込まれ事故、道路の陥没、地盤沈下
	使用する材料が締固め回数管理に適している	含水量が多い	締固め回数が足りない	転落事故、道路の陥没、地盤沈下
		含水量が少ない	過転圧が生じる	ひび割れ、崩壊、基盤沈下
無線通信障害の発生	低い位置に高圧線等の架線がないか、基地、空港等が近くにないか確認	確認しない	通信障害が発生する可能性が高い	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
	ＴＳの視準が遮るような障害物等がないか確認	確認しない	TSから移動局に設置した追尾用全周プリズムへの視準が遮られる	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
	同じ施工範囲内を同時施工する建機の数を確認	二台以上	TSが追尾すべき移動局とは別の移動局を誤って追尾する可能性がある。	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
	太陽フレアの発生時期	確認しない。	通信障害が発生する可能性が高い	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
GNSSの測位状態の問題	FIX解となるのに必要な衛星補足数が確保できる状況か確認	衛星からの電波がさえぎられる	FIX解得られない	作業中断になり事故はおこらない
	太陽フレアの発生時期	確認しない。	通信障害が発生する可能性が高い	建機の暴走による転落、衝突事故(周辺作業員、周辺住民)
	電波が多重反射	電波が多重反射	測位値に誤差	多重反射していると分かる前に衝突事故(運転手、周辺作業員、周辺住民)が生じる
精度の確認	TS測量機器が公称測定精度、最小目盛値を満たしているかどうか確認できる機器メーカ等が発行する書類があるか確認	確認しない	精度が確認できず誤差が生じる可能性がある	誤差の影響がある場合衝突事故の可能性
		確認したが書類がない	精度が確認できず誤差が生じる可能性がある	誤差の影響がある場合衝突事故の可能性
	既知座標とTSの計測座標が合致しているか	合致しない	機器の実際の位置をシステム上で把握することが難しい。締固め回数にずれが生じる。締固めを行う範囲を超える、足りない等の不備が生じ	衝突事故、転落事故。道路の陥没、地盤沈下、ひび割れ、崩壊
適切な表示判定	ローラまたは履帯が管理ブロック上を通過する毎に、当該管理ブロッ クが１回締固められたと判定し、車載モニタに表示	多く表示される	締固め回数が足りない	転落事故、道路の陥没、地盤沈下
		少なく表示される	過転圧が生じる	ひび割れ、崩壊、基盤沈下
	管理ブロック毎の累積の締固め回数が、車載モニタに表示	多く表示される	締固め回数が足りない	転落事故、道路の陥没、地盤沈下
		少なく表示される	過転圧が生じる	ひび割れ、崩壊、基盤沈下
	施工とほぼ同時に締固め回数分布図を画面表示	施工より早く表示	実際に施工されていない段階で施工されたことにされているため締固め回数足りない	転落事故、道路の陥没、地盤沈下
		施工より遅く表示	過転圧が生じる	ひび割れ、崩壊、基盤沈下
施工範囲の分割機能	施工範囲を、所定のサイズの管理ブロックに分割	所定のサイズより大きい	締固め不十分な場所が生じる。	転落事故、道路の陥没、地盤沈下
		所定のサイズより小さい	場所により過転圧が生じる。	ひび割れ、崩壊、基盤沈下、転落事故
締固め幅設定機能	締固め幅を、使用する重機のローラまたは履帯幅に応じて任意に設定	所定のサイズより大きい	締固め不十分な場所が生じる。	転落事故、道路の陥没、地盤沈下
		所定のサイズより小さい	場所により過転圧が生じる。	ひび割れ、崩壊、基盤沈下、転落事故
オフセット機能	締固め機械の位置座標取得箇所と実際の締固め位置との関係をオフセ ットする	機器ごとによって設定方法を変えていない	取得した位置座標と実際の締固め位置にずれが生じ、場所により品質に差が生じる。	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故
		前進、後進の認識ができていない	取得した位置座標と実際の締固め位置にずれが生じ、場所により品質に差が生じる。	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故
システムの起動とデータ取得機能	データの取得・非取得を施工中適宜切り替える	切り替えられない	過転圧が生じる場合や、締固め回数が足りない場合がある	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故
	振動ローラの場合は、有振時のみの位置座標を取得する	締固めしているときに非取得	実際の締固め回数とのずれが生じる。	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故
		締固めしていない移動時に取得	過転圧が生じる。	ひび割れ、崩壊、基盤沈下
締固め層厚分布図作成機能	締固め層厚分布図が作成	取得するデータが実際の標高データより大きい	締固め回数が足りないと判断され過転圧が生じる	ひび割れ、崩壊、基盤沈下
		取得するデータが実際の標高データより小さい	過転圧が生じたと誤認識	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故
座標取得データの選択機能	FIX解でのデータのみを取得する機能を有するか確認	FIOAT解も含まれる	誤差が生じ、過転圧が生じる可能性や締固め回数が足りない場所が生じる可能性がある	転落事故、道路の陥没、地盤沈下、ひび割れ、崩壊、基盤沈下、転落事故

【前提条件の整理】
検討の前提条件として、対象システムの概要やシステムモデル、要求仕様を整理した。前提条件については、STAP実施初期段階で整理するだけでなく、検討を進める過程で都度必要に応じて最小限の前提を策定した。STPA実施にあたっては、既往研究にて整理されている作業フロー[6]およびISO規格に掲載されている車両系建設機械の制御システムモデル[7]などを参考に、対象とする制御システムのモデル化、および当該制御システムが対象とする作業項目の洗い出しおよび整理を行った。本検討では「自動運転する油圧ショベルによる盛土工事」において、車両系建設機械が目標地点に移動し、盛土材を運搬・移動・放土する過程の制御を行う制御システムを対象とした。

【Step0(準備①)】
STPA実施にあたっては、対象システムにおいて「そもそも何が望ましくない事象なのか」などの状況を事前に定義しておく必要がある。本検討では労働安全衛生リスクを念頭においた分析を実施する観点から、アクシデントを「労働者の死傷を伴う事故」と定義し、これに従ってハザード（アクシデントにつながるようなシステムの状態もしくは条件）分析を行った。

【Step0(準備②)】
対象システムのうち、制御システムに着目して制御構造図（コントロールストラクチャー）を作成した。まず、自動運転する油圧ショベルによる盛土材の調達・運搬作業を対象に、制御システム内に出現する制御装置（コントローラ）および制御対象となるハードウェアシステム側のプロセス（被コントロールプロセス）について整理した。次に、当該システムの作業・制御フローを参考に、データおよび情報の流れを整理した。最後に、コントローラおよび被コントロールプロセスに関わる制御信号やデータを中心に、それらの関係性を整理したコントロールストラクチャーを構築した（図6）。図中のCAはコントロールアクションと呼ばれ、コントローラから被コントロールプロセスに向かって行われる制御指示のことである。

【Step1：非安全なコントロールアクション（UCA）の抽出】
構築したコントロールストラクチャーを基に、「コントローラにとっては正常にCAが行われるにも関わらず、その他の何らかの異常によりハザードに繋がるような事象（UCA）」を抽出した。ここでは検討の網羅性を高めるため、STPA手法に用意されているガイドワード（表5）を思考のきっかけとして用いて、ブレインストーミング式にUCAの抽出を行った。UCAを抽出した結果を表6に示す。例えば、コントローラからアクチュエータへの加速指示の信号が「与えられるとハザード」になる場合として、車両が静止した状態でいるべきときに信号を受信する場合が考えられ、これがUCAとして抽出される（UCA-P-1）。他のCAについても同様に検討することで、UCAを抽出した。

【Step2：ハザード要因の特定】
Step1で抽出した各UCAについて、それらがなぜ起きるのか、原因となるハザード要因（HCF）を特定した。ここではStep1と同様に、STPA手法に用意されているガイドワード（図7）を思考のきっかけとして用いて、ブレインストーミング式にHCFを特定した。HCFを特定した結果を表7に示す。例えば、前述の非コントロールアクション（UCA-P-1）が生じた場合、「(1)コントロールの入力か外部情報が欠けているか間違っている」すなわち、「その他外環境計測データに不備がある」ことがその原因の1つである可能性があり、これがHCFとして特定される。他のHCFについても同様に検討することで、HCFを特定した。

F. 結論と次年度に向けた課題・実施項目
本研究の目的は、自動制御システム等による車両系建設機械と協働する場合に新たに生じる労働安全衛生リスク分析フレームの構築である。初年度においては、自動運転する油圧ショベルによる盛土材運搬作業を対象としたHAZOP、作業HAZOPおよびSTAMP/STPAを実施することにより、油圧ショベルと周辺労働者が共存する環境下におけるハザードを体系的に特定した。
次年度は、特定されたハザード・リスクについての定量分析を志向したモデルベースアプローチを導入し、車両系建設機械の物理モデルおよび制御モデルを活用したリスク分析手法について検討を行う予定である。

G. 健康危険情報
特になし

H. 研究発表
特になし

I. 知的財産権の出願・登録状況
特になし

J. 参考文献

[1]. N. G. Leveson, Engineering a Safer World, System Thinking Applied to Safety, The MIT Press (2011)
[2]. (独)情報処理推進機構, はじめてのSTAMP/STPA～システム思考に基づく新しい安全性解析手法～ Ver.1.0 (2016)
[3]. ISO 26262-2:2018, Road vehicles – Functional safety – Part 2: Management of functional safety (2018)
[4]. JIS C 61882:2023, ハザード及び運用性の検討（HAZOPスタディー）―適用の指針 (2023)
[5]. 国土交通省, TS・GNSSを用いた盛土の締固め管理要領(2020)
[6]. S. Dadhich, et al., Key challenges in automation of earth-moving machines, Automation in Construction, Vol. 68, pp. 212-222 (2016)
[7]. ISO 15143-1:2010, Earth-moving machinery and mobile road construction machinery – Worksite data exchange – Part 1: System architecture (2010)

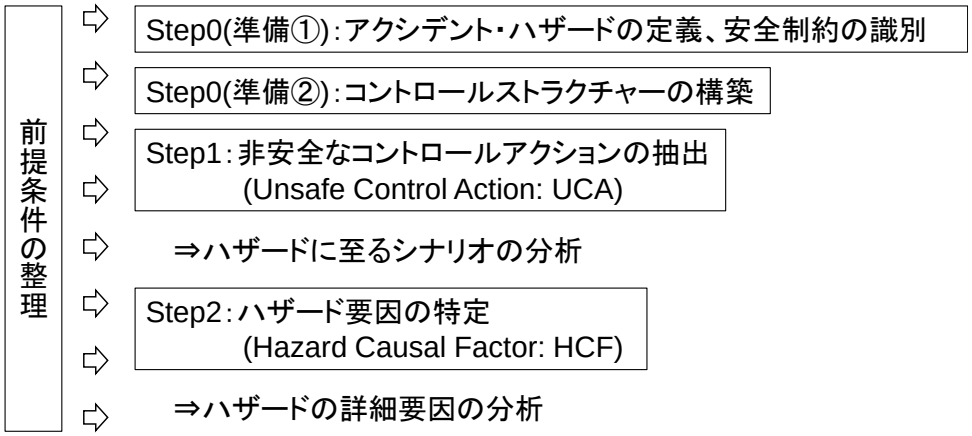

図 5　STPA 実施手順[2]

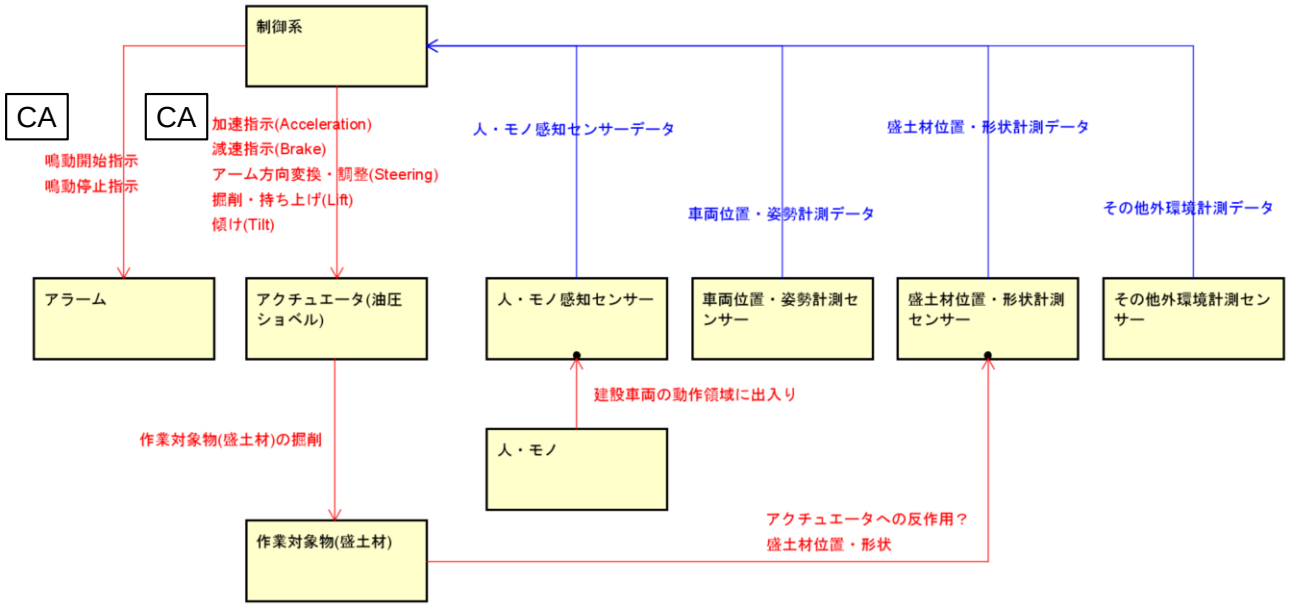

図 6　油圧ショベルによる盛土材の運搬作業を
対象としたコントロールストラクチャー

表 5　使用したガイドワード[2]

ガイドワード例	意味
与えられないとハザード (Not Providing)	安全のために必要とされるコントロールアクションが与えられないことがハザードにつながる。
与えられるとハザード (Providing causes hazard)	非安全なコントロールアクションが与えられることがハザードにつながる。
早過ぎ、遅過ぎ、誤順序でハザード (Too early/too late, wrong order causes hazard)	安全のためのものであり得るコントロールアクションが、早すぎて、遅すぎて、または順序通りに与えられないことでハザードにつながる。
早過ぎる停止、長過ぎる適用でハザード (Stopping too soon/applying too long causes hazard)	(連続的、または非離散的なコントロールアクションにおいて)安全のためのコントロールアクションの停止が早すぎる、もしくは適用が長すぎることがハザードにつながる。

表 6　非安全なコントロールアクション（UCA）の抽出結果（赤字）

No	CA	From	To	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	加速指示 (Acceleration)	制御系	アクチュエータ (油圧ショベル)	建設車両が静止した状態を維持し、建設作業が進まないが、保安上の懸念は少ない。	(UCA1-P-1) 建設車両が静止した状態でいるべきときに加速開始する。 (UCA1-P-2) 建設車両の動作中に、減速すべきときに加速開始する。	(UCA1-T-1) 建設車両が静止した状態から想定より早く加速開始する。 建設車両が静止した状態から想定より遅く加速開始するが、保安上の懸念は少ない。 (UCA1-T-2) 建設車両が静止した状態から直前の手順の前に加速開始する。 建設車両が静止した状態から直後の手順の後に加速開始するが、保安上の懸念は少ない。 (UCA1-T-3) 建設車両が静止した状態から想定より速いペースで加速開始する。 建設車両が静止した状態から想定より遅いペースで加速開始するが、保安上の懸念は少ない。	建設車両の動作中に加速が終わり、減速して停止するが、保安上の懸念は少ない。 (UCA1-D-1) 建設車両の加速開始後も加速し続け、減速・停止すべき地点で停止できない。
2	減速指示 (Brake)	制御系	アクチュエータ (油圧ショベル)	(UCA2-N-1) 建設車両が停止せず、労働者と接触・衝突する	建設車両が動作しないが、保安上の懸念は少ない。	建設車両が想定より早く停止し、目標位置に到達できないが、保安上の懸念は少ない。 (UCA2-T-1) 建設車両が想定より遅く停止し、停止する前に労働者と接触・衝突する。 建設車両が前の手順に先んじて停止し、目標位置に到達できないが、保安上の懸念は少ない。 (UCA2-T-2) 建設車両が次の手順の後で停止し、停止する前に労働者と接触・衝突する。	(UCA2-D-1) 建設車両の動作が停止しきらず、動作し続け、労働者と接触・衝突する。 建設車両が動作せず、作業が進まないが、保安上の懸念は少ない。
3	アーム方向変換・調整 (Steering)	制御系	アクチュエータ (油圧ショベル)	建設車両が方向変換せず、建設作業が進まないが、保安上の懸念は少ない。	(UCA3-P-1) 建設車両が方向変換において回転動作し続け、労働者と接触・衝突する。	(UCA3-T-1) 建設車両が想定より早く方向変換し始め、労働者が退避する前に労働者と接触・衝突する。 建設車両が想定より遅く方向変換し始めるが、保安上の懸念は少ない。 (UCA3-T-2) 建設車両が前の手順に先んじて方向変換し始め、労働者が退避する前に労働者と接触・衝突する。 建設車両が次の手順の後で動作し始めるが、保安上の懸念は少ない。	建設車両が想定より小さい範囲で方向変換を行い、建設作業が進まないが、保安上の懸念は少ない。 (UCA3-D-1) 建設車両が想定より大きい範囲で方向変換を行い、停止すべき位置で停止できない。
4	掘削・持ち上げ (Lift)	制御系	アクチュエータ (油圧ショベル)	アームおよびバケットが動作せず、建設作業が進まないが、保安上の懸念は少ない。	(UCA4-P-1) 建設車両が静止していない状態でアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。	(UCA4-T-1) 建設車両が静止する前にアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。 建設車両が静止した後にアーム及びバケットが動作するが、保安上の懸念は少ない。 (UCA4-T-2) 建設車両が静止する直前の手順の前にアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。 建設車両が静止した状態から直後の手順の後にアームおよびバケットが動作するが、保安上の懸念は少ない。	アームおよびバケットの動作量が不十分で、建設作業が進まないが、保安上の懸念は少ない。 (UCA4-D-1) アームおよびバケットの動作量が過剰となり、掘削量が過剰となり、建設車両が車体バランスを崩す。
5	傾け (Tilt)	制御系	アクチュエータ (油圧ショベル)	アームおよびバケットが動作せず、建設作業が進まないが、保安上の懸念は少ない。	(UCA5-P-1) 建設車両が静止していない状態でアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。	(UCA5-T-1) 建設車両が静止する前にアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。 建設車両が静止した後にアーム及びバケットが動作するが、保安上の懸念は少ない。 (UCA5-T-2) 建設車両が静止する直前の手順の前にアームおよびバケットが動作し、建設車両がバランスを崩し転倒する。 建設車両が静止した状態から直後の手順の後にアームおよびバケットが動作するが、保安上の懸念は少ない。	アームおよびバケットの動作量が不十分で、建設作業が進まないが、保安上の懸念は少ない。 (UCA5-D-1) アームおよびバケットの動作量が過剰となり、掘削量が過剰となり、建設車両が車体バランスを崩す。
6	鳴動開始指示	制御系	アラーム	(UCA6-N-1) 建設車両の想定動作領域内に労働者が入り込んでいるにも関わらず、アラームが鳴らない	建設車両の想定動作領域内に労働者が入り込んでいないにも関わらず、アラームが鳴るが、保安上の懸念は少ない。	建設車両の想定動作領域内に労働者が入り込む前にアラームが鳴ってしまうが、保安上の懸念は少ない。 (UCA6-T-1) 建設車両の想定動作領域内に労働者が入り込み、アラームが鳴る前に建設車両が動作してしまう。	(UCA6-D-1) 建設車両の想定動作領域内から労働者が退避していないにもかかわらずアラームが鳴りやんでしまう。 鳴動開始指示が継続し、鳴動停止指示が出ても鳴動し続けるが、保安上の懸念は少ない。
7	鳴動停止指示	制御系	アラーム	建設車両の想定動作領域内から労働者が退避してもアラームが鳴動し続けるが、保安上の懸念は少ない。	(UCA8-P-1) 建設車両の想定動作領域内から労働者が退避していないにもかかわらずアラームが鳴りやんでしまう。	(UCA8-T-1) 建設車両の想定動作領域内から労働者が退避する前にアラームが鳴りやんでしまう。 建設車両の想定動作領域内から労働者が退避した後でもアラームが鳴りやまないが、保安上の懸念は少ない。	建設車両の想定動作領域内から労働者が退避する前に鳴動停止指示が終わり、再度アラームが鳴動するが、保安上の懸念は少ない。 (UCA8-D-1) 鳴動停止指示が継続し、建設車両の想定動作領域内に労働者が入り込んでも鳴動しない。

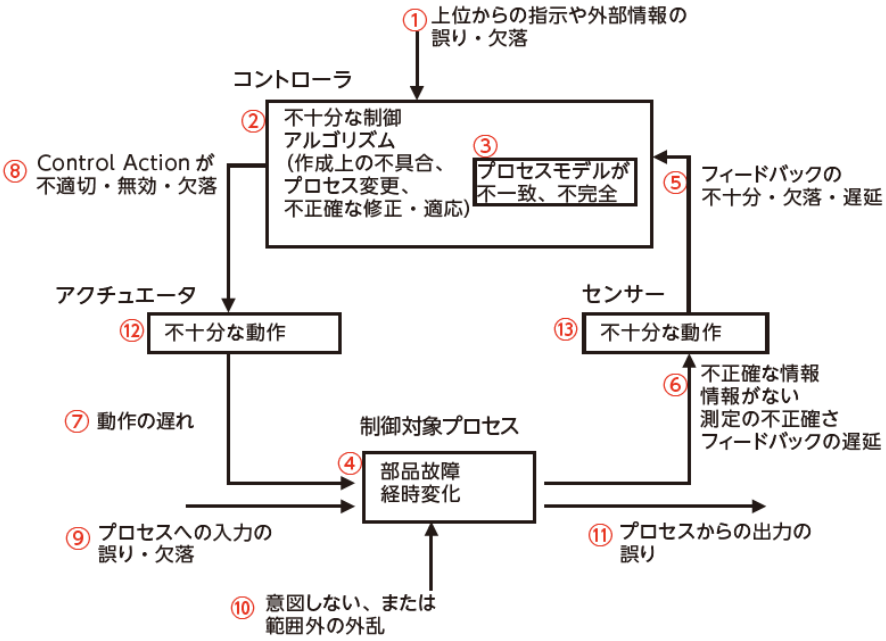

図 7　HCF 特定のためのガイドワード[2]

表 7　ハザード要因（HCF）の特定結果（一部）

ID	ヒントワード	HCF	シナリオ
HCF1-P-1-1	(1) コントロールの入力か外部情報が欠けているか間違っている	その他外環境計測データに不備がある	外環境の計測データが外乱等により不備があり、十分な外部情報が得られない状態で制御プロセスが加速開始を判断し、建設車両が人・モノに接触・衝突する。
HCF1-P-1-2	(2) コントロールアルゴリズムの生成の欠陥、プロセス変更、不正確な修正や適応	制御プロセスの設計ミス	制御プロセスの設計ミスにより、建設車両が意図せず加速開始し、建設車両が人・モノに接触・衝突する。
HCF1-P-1-3	(3) プロセスモデルの矛盾、不完全、不正確	制御プロセスモデルの設計ミス	制御プロセスの設計ミスにより、建設車両が意図せず加速開始し、建設車両が人・モノに接触・衝突する。
HCF1-P-1-4	(4) コンポーネント故障、経時変化	特になし	
HCF1-P-1-5	(5) 不適切か欠けているフィードバック、フィードバックの遅れ	人・モノ感知センサーから送られるデータに不備がある	建設車両の想定動作領域内に人・モノが入り込んでいることを制御プロセスが認識できず、建設車両が加速開始し、建設車両が人・モノに接触・衝突する。
HCF1-P-1-6	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	特になし	
HCF1-P-1-7	(7) 遅れたアクション	特になし	
HCF1-P-1-8	(8) 不適切、有効でない欠けたコントロールアクション	加速指示の不備	制御系が加速指示を出していないにも関わらず建設車両が加速開始し、周辺の人・モノに接触・衝突する。
HCF1-P-1-9	(9) プロセスへの入力が欠けているか間違っている	特になし	
HCF1-P-1-10	(10) 識別されないか範囲外の妨害	特になし	
HCF1-P-1-11	(11) プロセスの出力がシステムハザードの一因に	特になし	
HCF1-P-1-12	(12) アクチュエーターの不適切なオペレーション	加速指示がないままに、車輪が稼働する	制御系からの加速指示がないにもかかわらず、アクチュエーター（車輪）の不備によって車輪が稼働し、建設車両が移動し、人・モノに接触・衝突する。
HCF1-P-1-13	(13) センサーの不適切なオペレーション	各種センサーデータの不備	車両位置・姿勢計測センサーが正しく車両位置・姿勢を捉えられず、目標位置を正しく設定できず、目標位置を越えることで、人・モノに接触・衝突する。
HCF1-P-1-14	(14) 他のコントローラーとの通信が欠けているか間違っている	特になし	
HCF1-P-1-15	(15) 矛盾するコントロールアクション	特になし	