

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 環境情報研究院 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た。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

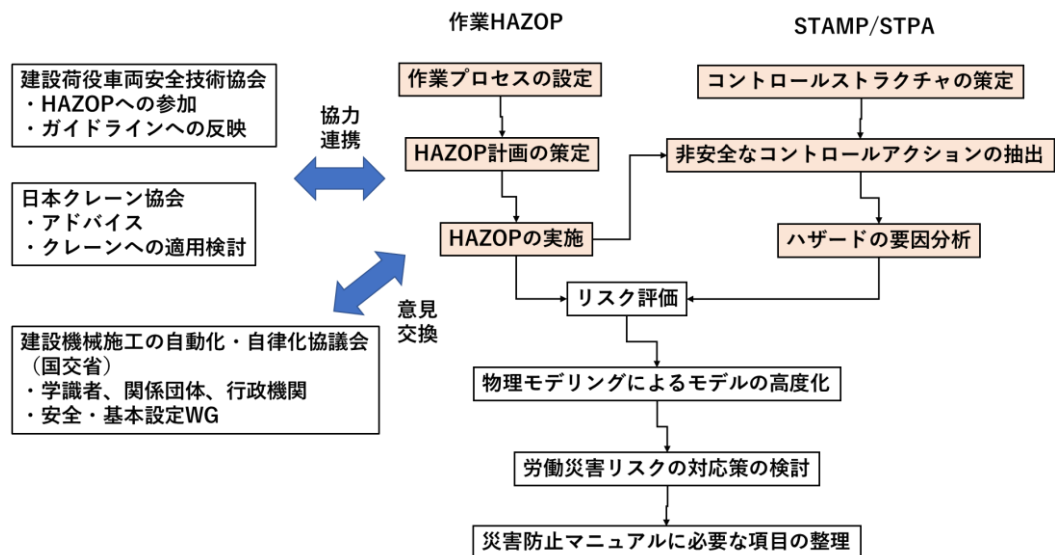


図1 本研究の全体像

得ない。そこで、次年度においては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、次年度実施項目として述べた、初年度実施のハザード分析の結果を活用した「モデルベースアプローチによる定量評価」の結果について述べると共に、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した結果について述べる。

C. モデルベースアプローチによるリスクシナリオの定量分析の試行

モデルベースアプローチとは、対象とする工学システムにおいて起こり得る物理現象のメカニズムに着目し、それを定式化して構築した「物理モデル」に基づいてリスク分析/評価を行うアプローチである。ここで「物理モデル」とは、本研究においては「複合物理領域・システムレベルモデリング[4]を用いて構築したモデル」を指す。当該モデリングは、機械系、熱系、電気系などの複数の物理領域に亘る現象を同一のプラットフォーム上で表現することが可能で、モデル解析および改変コストが比較的低いという特徴を持ち、近年では開発の短期化・効率化が求められる新規システムの設計開発プロセスとして普及が進められている「モデルベース開発プロセス」において汎用的に用いられているものである。これを実現するためのモデリング言語に、Modelica 言語 [5]がある。Modelica 言語は、マルチドメイン(複合物理領域)にわたるモデル化が可能なオブジェクト指向の物理モデリング言語の1種であり、複合物理分野が密接に関わり合ったプラントの物理モデルを作成することができる。物理領域の種類としては機械・電気・流体(気・液)・熱・制御など多岐にわたり、これらの各物理分野における現象を記述する基礎的な物理方程式を連立させることでモデル化を行う。

本研究では、以下の流れで当該モデリングに基づくリスクシナリオの定量分析を試行した。まず、前年度に実施したハザード分析およびリスクシナリオ特定 (HAZOP・作業 HAZOP・STPA) により特定されたリスクシナリオの中から、定量分析の対象としてより検討重要度の高いリスクシナリオを選定し、当該シナリオの状況を再現可能な物理モデルを構築した。次に、当該物理モデルを用いて、対象としたリスクシナリオの原因となるずれを与えた際の経時変化をシミュレーションすることで、当該リスクシナリオにおける車両系建設機械の物理的挙動を取得した。最後に、リスク分析に向けた情報取得として、分析対象リスクシナリオの影響を可視化することを試みた。車両系建設機械と労働者を模擬した立体モデルとの接触判定を元にリスクシナリオの影響を分析し、リスク分析/評価に向けた情報として整理した。

(ア) 分析対象シナリオの選定

前年度実施したリスクシナリオ特定の結果から、以降の定量分析を実施する対象としてより検討重要度の高いと考えられるリスクシナリオを選定した。本検討では、建設車両別事故統計において特に事故件数が多く見受けられた「油圧ショベル」が関わるプロセスとして、「油圧ショベルが盛土材付近の目的位置まで移動し、盛土材を掘削、その後旋回して放土する」プロセスに対してずれを想定し、そのずれを要因として生じる「油圧ショベルの異常動作によって周辺の労働者が死傷する」というリスクシナリオ特定結果を用いることとした。

(イ) 物理モデル構築

分析対象リスクシナリオ発生時の物理的環境として油圧ショベルとその周辺状況を再現するにあたり、物理領域として機械系および制御系を選定した。当該モデリング手法により構築した物理モデルを図2に示す。また、これらを簡易的に3次元にて可視化したものを図3に示す。物理モデリングソフトウェアとしては SimulationX 2024 を用いた。

機械系としては、油圧ショベルおよびダンプの物理構造として車体や荷台、キャタピラ部、アーム部、バケット部などについて考慮し、それらの駆動

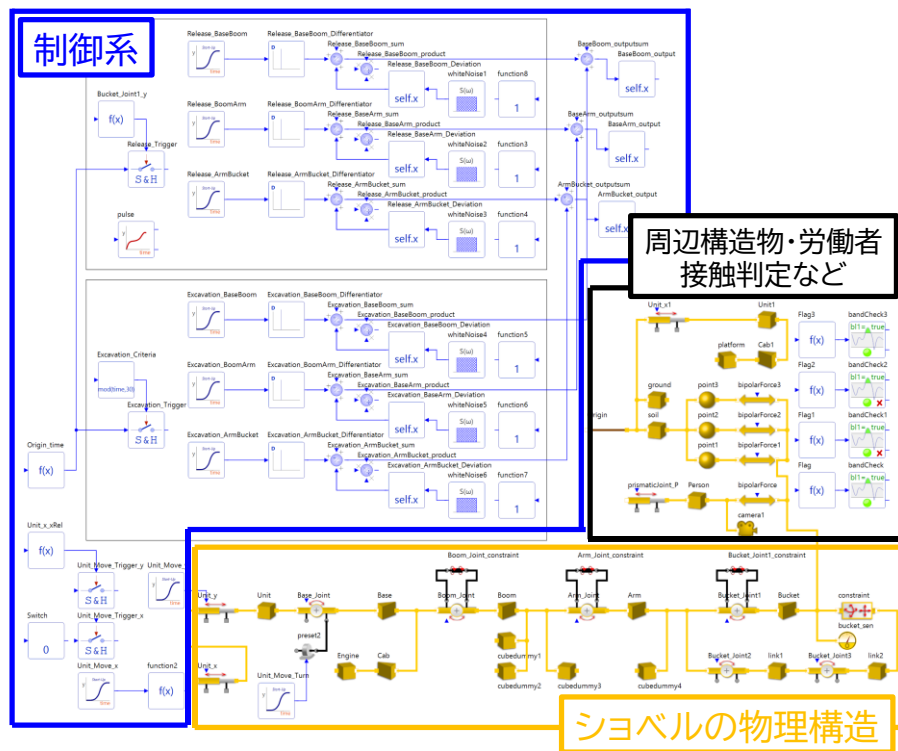


図2 物理モデリング手法を用いて構築した油圧ショベルの機械および制御モデルの概観

範囲についても設定した。油圧ショベルの脇に位置する盛土材を模擬した領域から盛土材を掘削し、ダンプの荷台に積み込む状況を想定した。制御系としては、主に油圧ショベルのアームによる掘削およびベースによる旋回動作を再現できるよう、各駆動部の駆動速度を適切に設定した。また、ここでは油圧ショベルの制御系に対して、分析対象リスクシナリオにおける「ずれ」を解析初期条件として入力できるようにした。

また、検討対象リスクシナリオの最終事象である「建設車両と労働者の接触による死傷」に着目し、建設車両と周辺の労働者の接触判定機構をモデル化することで、当該シナリオの影響を可視化することを試みた。建設車両周辺の労働者を模擬した立体モデルを物理モデル内に導入し、それぞれの中心点どうしの物理的距離をモニタリングすることで、シミュレーション中のある特定の時間における油圧ショベルと労働者の接触有無を判定でき

るように工夫した。

(ウ) リスクシナリオの定量分析

構築した物理モデルを用いて、リスクシナリオの定量分析を試行した。解析条件としては、油圧ショベルが初期位置から盛土材を掘削し、旋回してダンプに放土して初期位置に戻るまでの時間を30sと仮定し、その繰り返し動作を複数回実施させるために、解析時間は120sとした。また、環境の微細な変化や制御系のノイズをモデル化するため、油圧ショベルの制御系には分析対象リスクシナリオのずれとは別にホワイトノイズを与えた。

1つ目の事例として、「油圧ショベルの想定動作領域内に労働者が侵入し、ショベルに接触し死傷する」シナリオの定量分析を試行した(図4)。通常動作している油圧ショベルに対して労働者が低速(3cm/sと仮定)で接近し、あるタイミングで油圧ショベルの動作領域内に侵入してしまう状態を模擬した。グラフ(4-a)は油圧ショベルのアームおよびバケットの駆動角度を正規化した値の経時変化を表している。当該シナリオにおいては油圧ショベル側には特にずれを与えていないため、120s後までの全4サイクルについてほとんど同様の挙動を示している。グラフ(4-b)は、油圧ショベルのバケット中心と労働者立体モデル中心との距離による接触判定結果を表している。ここでは、両者の距離がゼロ(縦軸の判定値が1)になった瞬間に接触したと判定され、例えば約60s時点と他3つの時点で接触判定がなされていることがわかる。

2つ目の事例として、「センサー異常等によりショベルが想定動作領域を超え、労働者に接触し死傷する」シナリオの定量分析を試行した(図5)。通常動作している油圧ショベルの制御系に対して、あるタイミングで何らかの要因により異常なパルス信号が加わり、油圧ショベルが想定動作領域を超えてしまう状態を模擬した。グラフ(5-a)は(4-a)と同様の経時変化を表している。当該シナリオに

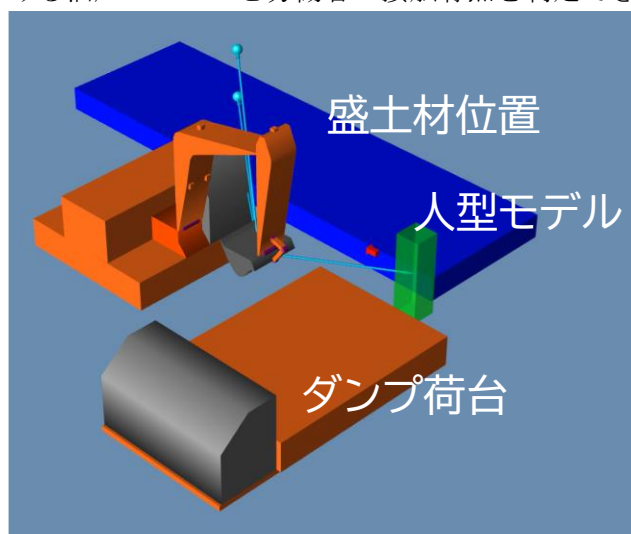
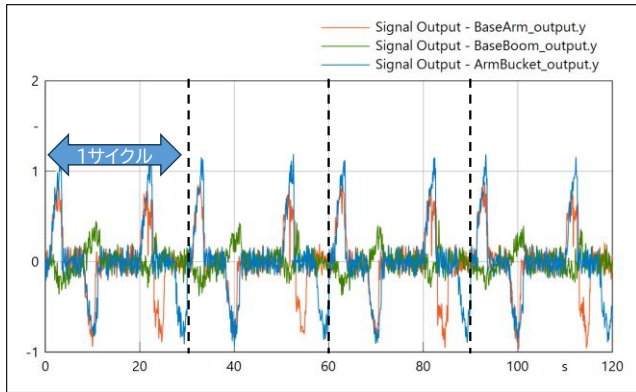


図3 3次元モデル概観

(4-a)アーム・バケット動作



(4-b)接触判定結果

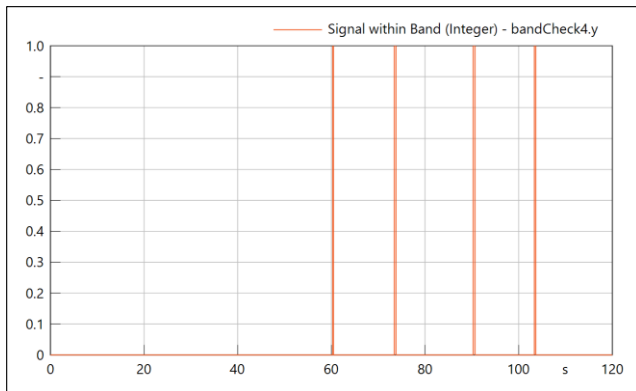


図4 「油圧ショベルの想定動作領域内に現場作業者が侵入し、ショベルに接触し死傷する」リスクシナリオの接触判定例

においては油圧ショベルの制御系に対して、約70s時点でパルス信号を与えているが、120s後までの全4サイクルについては目立った挙動の変動はないことがわかる。グラフ(5-b)は(5-a)とは異なり、縦軸は「バケット中心と人型モデル中心との距離」を表しており、パルス信号を与えた約70s以降のサイクルの挙動には変化がみられる。しかし、このケースでは当該距離がゼロになることはなく、「接触しない」と判定されていることがわかる。

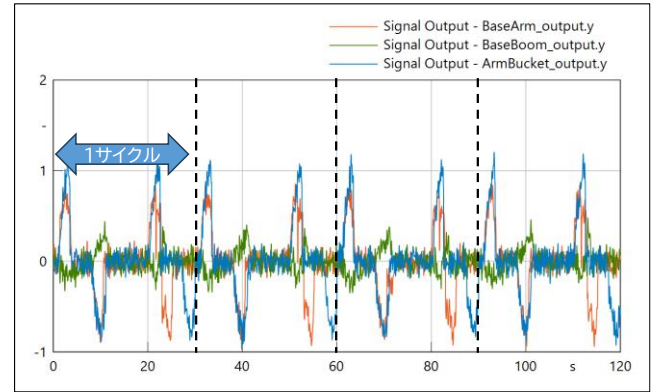
このように、様々なリスクシナリオの状況を踏まえて物理モデルを構築、シミュレーションを実施することにより、HAZOPやSTPA等で特定された定性的なリスクシナリオに対して定量的な情報を付与することができる。

D. 労働安全衛生リスク分析フレームの整理

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について、前年度および今年度に検討したハザード分析、リスクシナリオ特定、およびその詳細定量分析事例の検討結果を踏まえて、これらを当該リスクの分析フレームとして整理した。

図6に、本研究で対象としたリスクシナリオを分類した概念図を示した。本研究では、取り扱うリスクシナリオの原因系として、「車両系建設機械に由来するもの」「労働者に由来するもの」「両者の協働に由来するもの」の3種類に分類した。そして、これらの原因系に適用可能なハザード分析およびリスクシナリオ特定手法として、HAZOP、作業HAZOP、STPAを選定した。車両系建設機械に由

(5-a)アーム・バケット動作



(5-b)接触判定結果(バケット中心と人型モデル中心との距離)

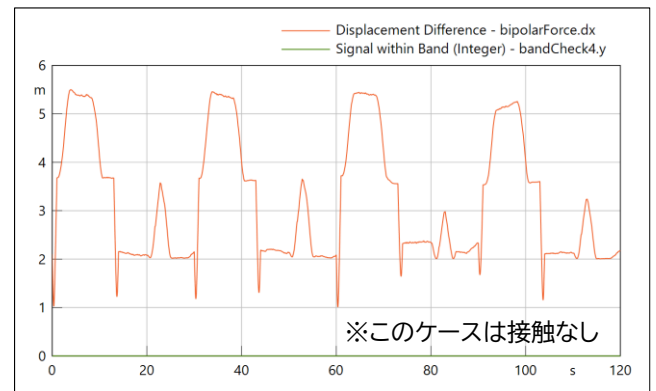


図5 「センサ異常等によりショベルが想定動作領域を超え、現場作業者に接触し死傷する」リスクシナリオの接触判定例

来するリスクシナリオの原因系は大きく「ハードウェア由来のもの」と「ソフトウェア由来のもの」に分けて考えることができ、その双方をHAZOPが、ソフトウェア由来のものの一部をSTPAが担うことができると考えた。また、STPAのアウトプットは「リスクシナリオが発現する条件(ハザード)」であるため、それがリスクシナリオとして顕在化する際の環境条件として、労働者の関与や外環境からの影響を加味することで、ソフトウェア由来のリスクシナリオおよび車両系建設機械と労働者の協働に由来するリスクシナリオを特定することができると考えた。さらに、労働者に由来するリスクシナリオとしてはその「作業手順」に着目し、作業が適切になされなかった場合のリスクシナリオの特定に作業HAZOPが適用可能であると考えた。そして、このリスクシナリオ分類および各手法により特定されたリスクシナリオについて、モデルベースアプローチを活用した詳細分析を実施することで、リスク分析のなかでも特に影響分析に必要な情報の取得が可能であると考えた。

なお、本フレームはリスクシナリオの分類およびそのリスク分析の一部の試行結果に基づくものに留まるものであり、これをもって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生じる「全ての」労働安全衛生リスクが分析できると考えることはできない点に注意が必要である。したがって、今後はさらなる事例検討および当該フレームの妥当性検証が必須である。

E. 労働災害防止マニュアルへの追加必要項目の

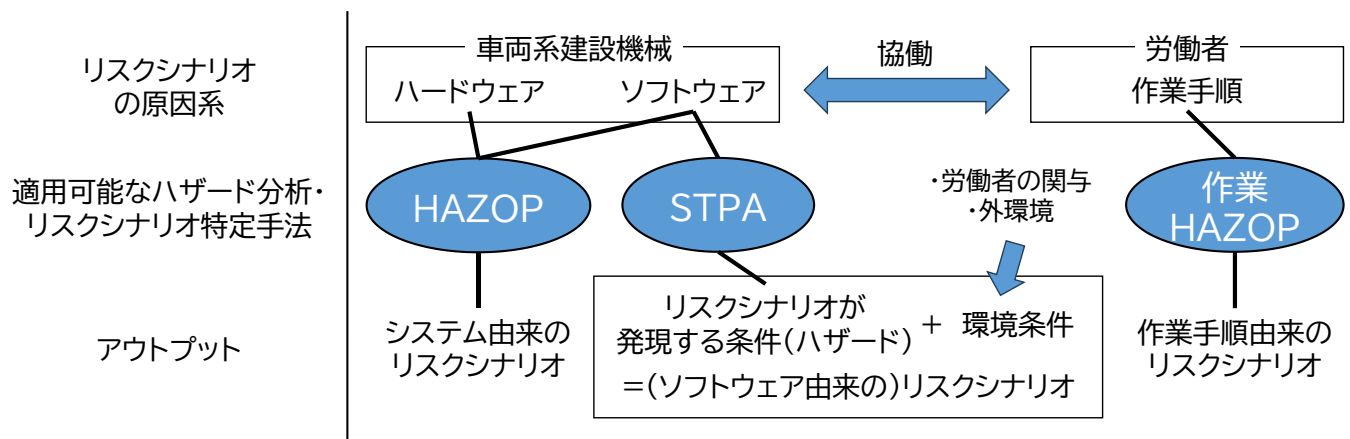


図6 自動制御システム等による車両系建設機械と労働者の協働により生じる労働安全衛生リスクシナリオの分類

整理および提案

(ア) 自律車両型建設機械の労働災害防止マニュアルに必要な項目

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した。令和6年3月に国土交通省より発行された自動施工における安全ルール(Ver. 1.0) [6]を対象に、各項目について検証を行った。

本研究では、労働災害被災リスクの定義を「人に危害を及ぼすリスク」に限定して検討を行う。具体的に対象とした事象を以下に示す。

- ① 自律建設車両と作業者の接触
- ② 自律建設車両と他の建設車両との接触（運転員の負傷）
- ③ 作業環境の悪化（長期暴露の影響）

(イ) 自動施工における安全ルール(Ver. 1.0)の概要

自動施工において、体系的に整理された安全方策を提示することで、自動施工における安全方策検討の効率化や、安全方策実施の適切化を図り安全を確保することを目的としている。自動施工における安全ルールの構成を以下に示す。

- ① 本ルールの役割、位置づけ
- ② 用語の定義
- ③ 安全性確保のための関係者の役割及びリスクアセスメント
- ④ 自動施工における安全方策
- ⑤ 自動建設機械や設備に求める安全方策に必要な機能

箇条3では、関係者の役割及びリスクアセスメントについて解説している。箇条3.3 リスクアセスメントでは、リスクアセスメントに関する留意点が述べられており、実施に当たってはISO12100 (JIS B 9700) が適宜参照される。

リスク特定では、当該施工現場における地形や天候などの環境条件、自動施工に関する施工計画、自動建設機械の特性や安全関連機能などを踏まえ、人に危害を及ぼすリスクが抽出、特定される。

箇条4で整理されている「自動施工における安全方策」を、表に示す。エリアの設定段階では、エリアの設定、面積、区割の他、(1)逸脱・侵入防止対策、(2)接触防止対策、(3)エリアの監視、が挙げられている。箇条5「自動建設機械や設備に求める安全方策に必要な機能」に示す機能は、それぞれの対

策に有効なものであり、必須もしくは推奨される機能となっている。

表1 自動施工における安全方策（エリア設定段階）

安全方策	自動建設機械や設備に求める安全方策に必要な機能
逸脱・侵入防止対策	(1) 自動建設機械の非常停止システム、(2) エンジン始動・停止と非常停止システム、(3) 自動建設機械の自動停止、(4) 表示灯の具備、(5) 自動と搭乗の切替スイッチ他、(6) 人・障害物検知機能、(7) 無線通信網
接触防止対策	(1) 自動建設機械の非常停止システム、(2) エンジン始動・停止と非常停止システム、(3) 自動建設機械の自動停止、(4) 表示灯の具備、(5) 自動と搭乗の切替スイッチ他、(6) 人・障害物検知機能、(7) 無線通信網
エリアの監視	(4) 表示灯の具備、(6) 人・障害物検知機能、(7) 無線通信網

(ウ) リスク評価に関する整理

自律建設車両においては、センサー等により周辺環境、システムの稼働状況について把握して、システムを制御している。このため、センサー、制御機器については、機能安全評価を行う必要がある。

自律建設車両の中核要素であるソフトウェア部についても適切なリスク評価が求められる。一方、自律システムを実現するソフトウェアを対象としたリスク評価手法については、十分に確立していないため、ソフトウェアの検証と妥当性確認が必須である。とくに、リスク分析者が論理システムを把握している従来のアルゴリズムの評価とは異なり、ブラックボックス化したソフトウェアの妥当性を確保するためのフレームを構築することが求められる。

自律システムと機械システムのインターフェースにおいて考慮すべきリスクを特定、分析、評価する必要がある。本研究で実施した、機械システムとソフトウェア部両方を対象とするHAZOPや

STAMP/STPA 等を用いたプロセスに着目したリスク分析技術の導入が望ましい。

(エ) リスク評価に基づく労働災害防止対策

本研究で実施された HAZOP 及び STPA の分析では、ソフトウェア部の不具合に起因した労働災害シナリオが多く特定されている。建設車両は、自主検査等によりその性能が維持される。区分として、ブルドーザ・トラクター・ショベルでは

- ① エンジン
- ② 動力伝達装置
- ③ 走行装置
- ④ 制動装置
- ⑤ 作業装置
- ⑥ 油圧装置
- ⑦ 操作
- ⑧ 安全装置・車体関係等
- ⑨ 総合
- ⑩ 排ガス装置

があり、各項目について詳細な点検項目が定められている。一方、ソフトウェアの検査については、現在点検方法などは定められておらず、ソフトウェア不具合を起因とした労働災害の方策は確立していない。

作業者の確認事項として、運転開始前及び運転操作中の要求事項として以下のように整理した。

■運転開始前に、作業員は次の事項を確認しなければならない：

- 自律運転により制御される装置が車両制御に適合し、操作の承認を受けていること。
- 自律運転により制御される装置が正常に動作していること。
- 停止機能が正常に動作しており、意図する動きを制御する準備が整っていること。
- 自律運転により制御される装置のすべてのコントロールが中立位置にあること。

■自律運転操作中、作業員は次の事項を確実にしなければならない：

- 自律運転により制御される装置が意図した機械と通信していること。
- 操作中の車両または車両群の意図する動きが作業員とは別に監視されていること。
- 監視員が安全な位置で気を散らすことなく監視していること。
- 監視員が意図する動きについて直接観察するか、現場から指示を受け取ることができること。
- 短時間の非使用または意図する操作が完了した後、自律運転により制御される装置をオフにすること。

これらの事項は、本研究で実施されたリスク分析の結果をベースに検討したものであるため、前提条件が限られている。今後より幅広くリスク分析を行い、現行の労働災害マニュアルとの差分を明確にしていく必要がある。

F. 結論

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。今年度においては、初年度実施のハザード分析の結果を

活用した「モデルベースアプローチによる定量評価」の結果も踏まえて、自動制御システム等による車両系建設機械と労働者の協働により生じる労働安全衛生リスクの分析フレームを整理し、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した。

G. 健康危険情報

特になし

H. 研究発表

- (1) 出越恵大, 鈴木智也, 笠井尚哉, 酒井信介, 澁谷忠弘, HAZOP を用いた自律型建設車両と現場作業者の協働における事故危険性の分析, 第 57 回安全工学研究発表会, 富山, Session 7, No. 19, 2024
- (2) 鈴木智也, 笠井尚哉, 酒井信介, 澁谷忠弘, STPA を用いた自律型建設車両と現場作業者の協働における労働安全衛生リスク分析, 第 57 回安全工学研究発表会, 富山, Session 11, No. 35, 2024

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]. 大島明, 複合物理領域モデリング, 計測と制御, 53, 4 (2014)
- [5]. Peter Fritzson, Modelicaによるシステムシミュレーション入門, TechShare (2015)
- [6]. 国土交通省, 自動施工における安全ルール Ver.1.0 (2024)