様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 ２２ 日現在

機関番号：１３５０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ０４９２０

研究課題名（和文）ソフトウェアの相互作用に起因するハザード原因の複数の安全解析手法の連携による解析

研究課題名（英文）A study of analysis methods for a hazard that is resulted from interactions between software components by coordinating with multiple safety analysis method

研究代表者
高橋　正和（TAKAHASHI, MASAKAZU）

山梨大学・大学院総合研究部・教授

研究者番号：２０４０３４４６

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究では、システムのハザード解析手法の研究を行い、システムを安全化する方法を提案した．ハザードとはシステムの状態のことで、その状態を放置する、その状態で特別な条件が成立するとアクシデント（人、システム、環境等に悪影響を及ぼす）が発生する状態と定義する．本研究ではハザード解析に用いるFailure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Hazard and operability Study (HAZOP), System Theoretic Process Analysis (STPA)の各手法を提案した．

研究成果の学術的意義や社会的意義
本研究の成果により、システムに発生するハザードの要因を系統的に明確化する方法を確立することができた．特に、特徴の異なるハザード解析手法群を準備することができた．その結果、システムの目的に応じて、適切な手法を適用すること、あるいは、複数の手法を適用してシステムの生じるハザードを網羅的に検出し、その要因を明らかにできるようになった．このことにより、システム安全性を向上させることができるようになった．このことは、各種の社会基盤や工業製品の安全性を高めることになり、社会的な意義は大きい．

研究成果の概要（英文）：In this research, we researched a method of system hazard analysis and proposed a method of making a system safe. Here, a hazard is defined as a state of a system that will cause an accident (it causes negative impacts on people, systems, environment, etc.) when left unchecked or when special conditions are met in that state. In this research, we proposed hazard analysis methods, such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Hazard and operability Study (HAZOP), and System Theoretic Process Analysis (STPA).

研究分野：ソフトウェア工学

キーワード：STPA　HAZOP　FMEA　FTA　ハザード解析

１．研究開始当初の背景

はじめに，重要な用語を定義する．本研究ではハザードとは放置するとアクシデントに至る状態，あるいは，放置した際に特別な条件が成立するとアクシデントに至る状態と定義する．

さらに，アクシデントは人，工業製品，周囲の環境等に悪影響を与えることと定義する．近年，工業製品の高機能化や高性能化を実現するために組込みソフトウェア（Embedded Software: EBSW）を搭載し，高度な制御を行うことが主流となり，EBSW が複雑で大規模になった．その結果，EBSW のハザードにより，工業製品にアクシデントが生じ，社会的な問題となってきた．そのため，EBSW に生じるハザードの種類を明らかにするとともに，その原因を明らかにする方法が必要になってきた．しかし，今までに EBSW 向けのハザード解析の手法は定式化されていなかった．そこで本研究では，はじめに EBSW が適切な機能と性能を有していることを確認するために必要となるハードウェアと EBSW の結合テストを行う方法を研究する．さらに，複雑になった EBSW を構成する要素（コンポーネント）間に相互作用に基づいたハザードの解析手法について研究する．これにより工業製品の安全性の向上に貢献する．

２．研究の目的

本研究では，EBSW を搭載した工業製品の使用時に生じるハザードの原因を解析する方法を提案する．具体的には工業製品のハードウェアと EBSW の結合テストを網羅的に実施して，EBSW を含む工業製品の機能と性能の適切さを立証した上で，EBSW を構成するコンポーネントの相互作用に基づいて発生するハザード，および，その要因を明らかにする．前者については，EBSW で計測している物理量（センサーの値）が異常な値をとったときに工業製品がどのようなハザードを発生するのかを分析する Hazard and Operability Study (HAZOP)を用いて網羅的な結合テストのテストケースを生成する方法を提案する．後者については，工業製品を構成するコンポーネント間 の相互作用により発生するハザードの要因を分析する System Theoretic Process Analysis (STPA)を用いて，EBSW のコンポーネント間の相互作用に基づいたハザードの要因を明らかにできるようにする．さらに，網羅的に EBSW の生じる可能性のあるハザード及びその要因を網羅的に分析できるようにする．このことにより，安全な EBSW および工業製品を開発できるようにする．

３．研究の方法

本研究では HAZOP を用いたハードウェアと EBSW の結合テストのテストケースを網羅的に作成し，それを実施することで適切な機能と性能を有する EBSW を開発する．そして，STPA を用いて，工業製品を構成するコンポーネント（ハードウェア，EBSW）の相互作用により発生する可能性のあるハザードとその要因を分析する方法を研究する．

はじめに，HAZOP の研究について述べる．図１に提案手法の概要を示す．以下に提案手法を構成する作業について説明する．(1) 検証の対象となる工業製品のハードウェアとソフトウェアの設計仕様を入力として，HAZOP で使用するパラメータのファイルを定義する．(2) パラメータファイルと事前に定義しておいたガイドワードのファイルを組み合わせて工業製品のずれた状態を生成する．(3) 生成されたずれた状態を精査して，望ましくない事象を引き起こすずれた状態を選定する．これを結合テスト項目とする．(4) 結合テスト項目，ハードウェア設計情報，ソフトウェア設計情報を元に結合テストケースを生成する．(5) 結合テストケースを実行する．そして，(6) 結合テストケースの実

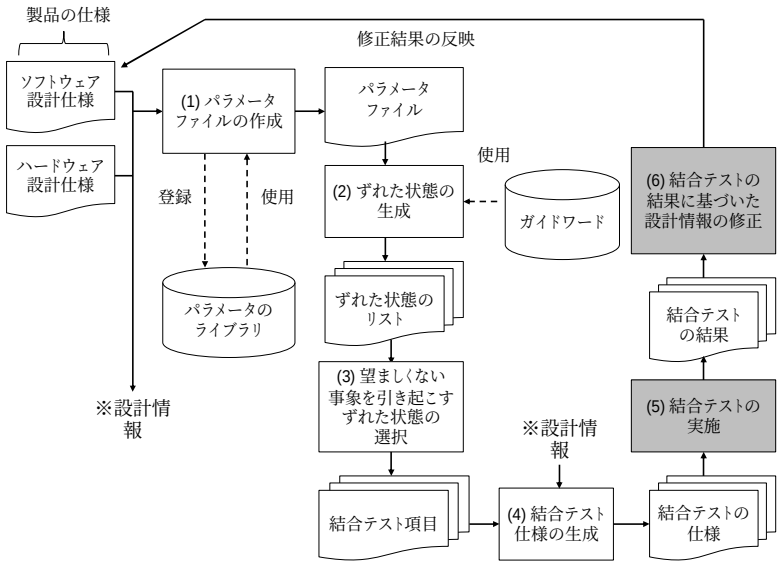

図１　HAZOP を用いた結合テストケース生成

行結果にもとづいて，ハードウェアとソフトウェアの設計仕様書の修正を行う．(1)から(6)の作業を繰り返すことで，適切な制御ソフトウェアを実現する．ただし，(5)と(6)は本成果報告の範囲外とする．

次に，STPA に工業製品を構成するコンポーネント間の相互作用により発生するハザードおよびその要因の分析方法ついて述べる．図２に STPA を用いた工業製品のハザード分析手法の概要を示す．以下に提案手法を構成する作業を説明する．(1) UML システム仕様の作成ではオブジェクト指向仕様記述言語 Unified Modeling Language (UML)を用いて EBSW の仕様(UML システム仕様．ユースケース図とクラス図から構成）を定義する．ユースケース図では EBSW と相互作用する他システムを定義する．クラス図では EBSW の機能構造（クラス構造）と各機能を実現するプログラム部位（メソッド）を定義する．(2) STPA を用いたハザードシナリオの作成では UML システム仕様を入力して STPA を実行し，ハザードシナリオを作成する．はじめにアクシデント，ハザード，安全制約を定義する．次に UML システム仕様からシステムの制御構造を表す Control Structure Diagram (CSD)を作成する．CSD の要素はアクターとクラスとする．要素間の Control Action (CA)はクラス間でのメソッド呼び出しとし，CA の方向はクラス間の誘導可能性と同方向とする．要素間の Feedback Data (FBD)はメソッドの戻り値とする．図３に UML システム仕様と CSD の対応関係の例を示す．三番目に CSD 中の CA と STPA で提案された「ハザードにつながる 4 種類のガイドワード」の全組み合わせの中から非安全な状態を引き起こす可能性のある Unsafe Control Action (UCA)を抽出する．四番目に UCA と CSD からハザードを引き起こす可能性のあるコントロールループを識別し，STPA で提案された「コントロールループ上の UCA が Hazard Causal Factor (HCF)となるかを判定する 11 種類のガイドワード」を当てはめ，ハザードを抽出し，その時の条件を明らかにしてハザードに至る過程をシナリオとして記述する．本課題では，CA や UCA

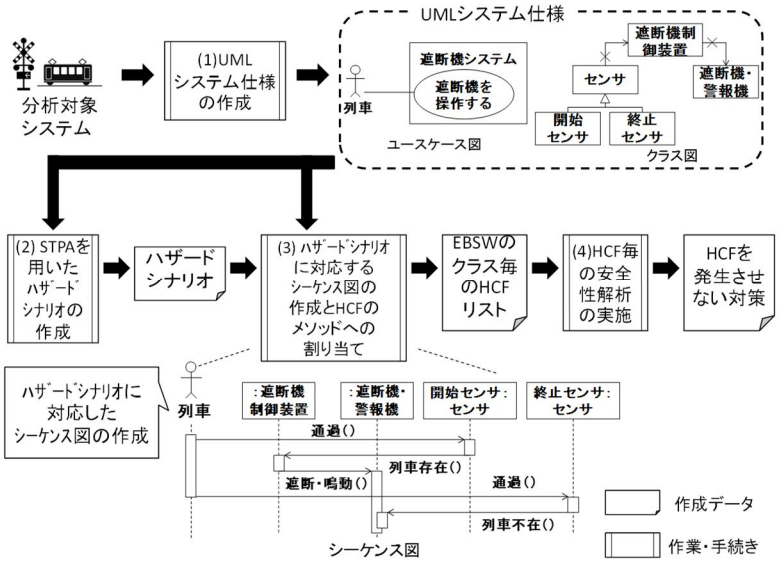

図２　STPA を用いたハザード解析手法の概要

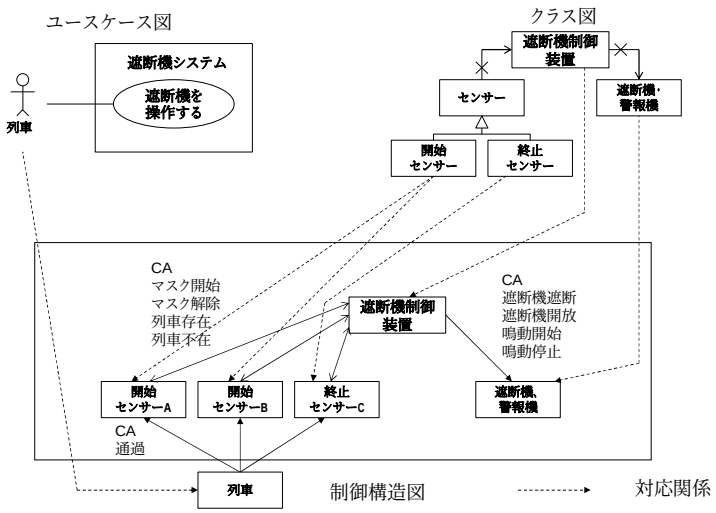

図３　UML システム仕様と CSD の対応関係

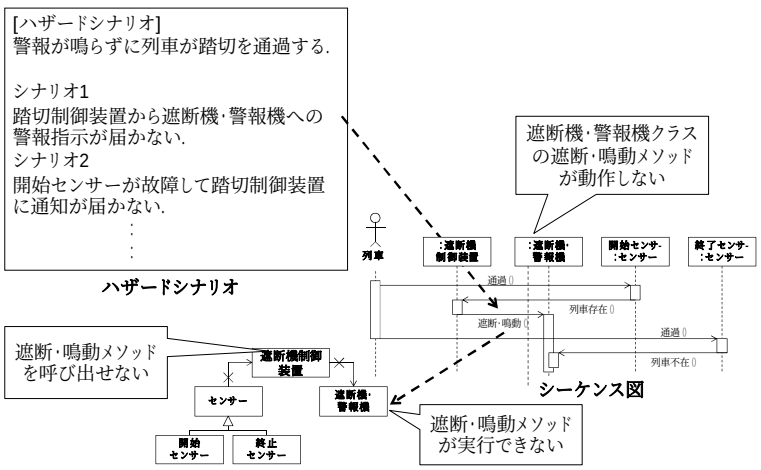

図４　メソッドとハザードの対応関係

とガイドワードを組み合わせて，その中から条件に合致したものを抽出する．そして(3) ハザードシナリオに対応するシーケンス図の作成と HCF のメソッドへの割り当てでは UML システム仕様とハザードシナリオから，ハザードシナリオに対応するシーケンス図を作成する．シーケンス図のライフラインはアクターとクラス，ライフライン間のメッセージは EBSW のクラスのメソッド，メッセージの向きはクラス間の誘導可能性と同方向とする．シーケンス図通りにメソッドが動作することでハザードが発生するので，各メソッドが動作する条件が HCF となる．図４にメソッドと HCF の関係の例を示す．そして，(4)で HCF 毎の安全性解析を実施して，ハザード要因を明確にするとともに，ハザードを発生させないための対策を立案してハードウェアおよび EBSW の仕様に反映させる．この作業を全ハザードシナリオに対して実施して全 HCF を明らかにする．

４．研究成果

はじめに HAZOP の研究に関する成果について述べる．提案手法を小型のロボットの動作の検証に使用した．その結果，提案手法で 74 個の結合テストケースを生成することができ，20 個のハザードとその要因を発見できた．このことから，手作業でテストケースを生成した場合と比較して 25%多くの有効なテストケースが作成でき，42%多くのハザードとその要因が発見できた．今回発見できたハザードの要因の一部は EBSW 単体のテスト，ハードウェア単体のテストの単体だけでは発見できないものであった．さらに，提案手法によりテストケースの生成に要する時間を約 25%削減することができた．以上の結果により，提案手法を用いることで，より多くの工業製品のハザードとその要因を発見することができるようになり，工業製品の品質を向上させることが可能になった．

次に STPA の研究に関する成果について述べる．提案手法を踏切遮断機制御システムのハザード解析に適用した．その結果，複数のハザードとその要因を明らかにすることができた．さらに，それを発生させないための対策を立案することができた．これにより，当該ハザードが発生するリスクを低減し，対象システムの安全性を高めることができた．一方，1 個のハザードに対して多数のハザードシナリオが考えられるため，効率的にハザード要因を分析する方法が必要であることが分かった．また，提案手法ではハザードシナリオ毎に対策を立案するので，対策の間に矛盾が生じる可能性が存在することが分かった．対策の間の矛盾を確認するための方法が必要になることも分かった．さらに，実際の対策を立案する場合には，安全性，費用，期間等を考慮したうえで，工業製品の使用方法に関する制約設定，ハードウェアの設計変更，EBSW の設計変更のいずれの方法で対応するのかを検討し，効果的に安全な仕組みを構築する必要がある．**以上の結果により，提案手法を用いることで，工業製品のハザードとその要因を発見と適切な対策が立案できるようになり，工業製品の品質を向上させることが可能になった．**

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　11件／うち国際共著　10件／うちオープンアクセス　4件）

１．著者名 Masakazu Takahashi, Yunarso Anang, and Yoshimichi Watanabe	４．巻 12(2)
２．論文標題 A Safety Analysis Method for Control Software in Coordination with FMEA and FTA	５．発行年 2021年
３．雑誌名 MDPI Information	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/info12020079	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Masakazu Takahashi, Kouji Ueno, Yunarso Anang, and Yoshimichi Watanabe	４．巻 2021
２．論文標題 A Comprehensive Creation Method of Hardware and Software Combined Test Specifications for Industrial Product Controlled by Software using HAZOP	５．発行年 2021年
３．雑誌名 Proc. of SICE2021	６．最初と最後の頁 443-448
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Masakazu Takahashi,Ueno, Yunarso Anang, and Yoshimichi Watanabe	４．巻 N/A
２．論文標題 Planning of the Hardware and Software Combined Test Cases for Industrial Product in the Abnormal Condition using HAZOP	５．発行年 2021年
３．雑誌名 Proc. of ISQFD2021	６．最初と最後の頁 25-34
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Masakazu Takahashi, Yunarso Anang, Yoshimichi Watanabe	４．巻 5
２．論文標題 A Hazard Analysis Method for Embedded Control Software with HAZOP	５．発行年 2020年
３．雑誌名 Computer Science and Information Technology	６．最初と最後の頁 82-96
掲載論文のDOI（デジタルオブジェクト識別子） 10.17352/tcsit	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Masakazu Takahashi, Yunarso Anang, Yoshimichi Watanabe	4．巻 12
2．論文標題 A Safety Analysis Method for Control Software in Coordination with FMEA and FTA	5．発行年 2021年
3．雑誌名 Information	6．最初と最後の頁 1-21
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/info12020079	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Masakazu Takahashi, Yunarso Anang, Yoshimichi Watanabe	4．巻 11
2．論文標題 A Proposal of Fault Tree Analysis for Embedded Control Software	5．発行年 2020年
3．雑誌名 Information	6．最初と最後の頁 1-22
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/info11090402	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Yoshimichi Watanabe, Masakazu Takahashi	4．巻 -
2．論文標題 A Proposal to Reliability Deployment of Embedded Software Adopting the STAMP Model in QFD	5．発行年 2019年
3．雑誌名 PROC. of ISQFD'19-Boise	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Masakazu Takahashi, Yunarso Anang, Yoshimichi Watanabe	4．巻 -
2．論文標題 A Merthod for Detecting Modified Code Clones in a Program	5．発行年 2019年
3．雑誌名 Proc. of IRSET2019	6．最初と最後の頁 106-116
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Masakazu Takahashi, Yunarso Anang, Yoshimichi Watanabe	４．巻 -
２．論文標題 A Proposal for a Hazard Analysis Method for Embedded Control Software Using STAMP	５．発行年 2019年
３．雑誌名 Proc. of SICE2019	６．最初と最後の頁 595-600
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yunarso Anang, Yoshimichi Watanabe, Masakazu Takahashi, et. al	４．巻 -
２．論文標題 Implementation of Computer-Based Test in Countrywide New Student Recruitment Process	５．発行年 2019年
３．雑誌名 Proc. of InCIT2019	６．最初と最後の頁 273-278
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Nuraiza Rahmadhanty, Yunarso Anang, Yoshimichi Watanabe, Masakazu Takahashi	４．巻 -
２．論文標題 An Assessment of the Survey's Officer Performance Using AHP	５．発行年 2019年
３．雑誌名 Proc. of ANQ2019	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　5件）

１．発表者名 Yoshimichi Watanabe
２．発表標題 A Proposal to Reliability Deployment of Embedded Software Adopting the STAMP Model in QFD
３．学会等名 ISQFD19'-Boise（国際学会）
４．発表年 2019年

１．発表者名
Masakazu Takahashi

２．発表標題
A Merthod for Detecting Modified Code Clones in a Program

３．学会等名
IRSET2019（国際学会）

４．発表年
2019年

１．発表者名
Masakazu Takahashi

２．発表標題
A Proposal for a Hazard Analysis Method for Embedded Control Software Using STAMP

３．学会等名
SICE2019（国際学会）

４．発表年
2019年

１．発表者名
Yunarso Anang

２．発表標題
Implementation of Computer-Based Test in Countrywide New Student Recruitment Process

３．学会等名
InCIT2019（国際学会）

４．発表年
2019年

１．発表者名
Nuraiza Rahmadhanty

２．発表標題
An Assessment of the Survey's Officer Performance Using AHP

３．学会等名
ANQ2019（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	渡辺　喜道 (Watanabe Yoshimichi) (00210964)	山梨大学・大学院総合研究部・教授 (13501)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関