情報処理学会論文誌 Vol.58 No.2 521–530 (Feb. 2017)

D-Caseを用いた安全分析結果の説明手法の提案

小林 展英[1,a)] 森崎 修司[1] 山本 修一郎[1]

受付日 2016年5月24日, 採録日 2016年11月1日

概要：現在，車載ソフトウェア開発では，HAZOP（Hazard and Operability Studies），FTA（Fault Tree Analysis）といった分析手法を用いて安全性を分析し，その結果に基づいて車載ソフトウェアの開発を進めている．ISO26262 の本格導入を想定すると，これに加えて開発した車載ソフトウェアの安全性を第三者に納得してもらうための安全性ケースの作成が必要になる．安全性ケースの作成には，記述品質の安定化を図るために，D-Case などの図式言語の採用が期待されるが，従来の D-Case 作成法では，HAZOP，FTA の分析結果を証拠として用いる，という分析過程が反映されない単純で間接的なガイドラインしか存在していなかった．このため，開発現場では具体的な安全分析結果に基づいた説明が間接的になるという問題があった．この問題を解決するためには，HAZOP，FTA と D-Case を対応づけるとともに，その手順を提示する必要がある．本稿では，外部と内部の視点，分析と確認の視点に基づいて，HAZOP，FTA，D-Case を対応づけた新たな組み合わせ手法を提案する．また，本手法を適用した実験結果に基づき，その有効性を確認する．

キーワード：D-Case，HAZOP，FTA，GSN，車載ソフトウェア

The Method of Explanation for Safety Analysis Results Using D-Case

Nobuhide Kobayashi[1,a)] Shuji Morisaki[1] Shuichiro Yamamoto[1]

Received: May 24, 2016, Accepted: November 1, 2016

Abstract: Mostly automotive software development has adapted HAZOP (Hazard and Operability Studies), FTA (Fault Tree Analysis) to analysis safety of its product, and has developed it based on the analysis results. Assuming full introduction of ISO26262, it is necessary to construct a safety case to convince stakeholders in actual development. It is expected to adapt graphical language such as D-Case to keep stable quality of a safety case. However, there is only simplified and indirect guideline of using the results of HAZOP and FTA as evidences in the conventional D-Case construction method. As a result, many actual development might have a problem that a relationship between analysis results and a safety case is indirect. For solving this problem, it is necessary to closely collaborate HAZOP, FTA and D-Case, and to also define the process of constructing D-Case using the collaboration. This paper proposes the method of collaborating HAZOP, FTA, and D-Case based on the view of external and internal, and the view of analysis and confirmation. Additionally, it confirms the effectiveness of the method on the basis of the case study.

Keywords: D-Case, HAZOP, FTA, GSN, automotive software

1. はじめに

車載ソフトウェア業界では，ISO26262 に対応した車載ソフトウェア開発手法の確立が急務の課題となっており，安全分析の領域については，従来から利用されている HAZOP，FTA が採用される可能性が高い．従来から行われてきた安全分析は，「利用者視点でのハザード抽出」，「開発者視点でのハザード要因の抽出」，「開発者視点での対策確認」の 3 つの工程に大まかに分けることができる．一方，ISO26262 を想定した安全分析では，「利用者視点での対策確認（第三者への説明）」を加える必要があり，この工程では上述した 3 つの工程のつながりや各工程で行われた判断の根拠を可

[1] 名古屋大学情報科学研究科
Information Science, Nagoya University, Nagoya, Aichi 464–8601, Japan
[a)] kobayashi.nobuhide@j.mbox.nagoya-u.ac.jp

視化することが求められる．参考文献 [1] の調査結果からも分かるとおり，HAZOP，FTA は分析手法として利用実績も高く，分析手法として有用であるが，これらの手法だけでは第三者への説明時に必要となる情報を可視化することは困難である．また，従来の開発現場における安全分析では，HAZOP，FTA の分析結果，およびその対策の確認結果を安全性ケースとして統合する手順が明文化されておらず，さらにその記述方法も自由記述の自然言語が採用されているため，安全性ケースの記述品質が分析者のスキルに大きく依存していた．

本稿では，「利用者視点での対策確認（第三者への説明）」に対して D-Case を採用し，上述したそれ以外の 3 つの工程で用いられる手法と対応づけた安全性ケースの作成方法を提案する．また，D-Case の自由度の高さに起因する記述品質の問題を，HAZOP，FTA と組み合わせることで解決する方法についても考察する．さらに，本手法を簡易的なヘッドライト制御システムに適用し，その結果に基づいた本手法の有効性について説明する．

なお，本章以降では，2 章で関連研究について述べ，3 章で本稿の提案手法について説明する．さらに，4 章で提案手法を適用した実験結果について述べ，5 章で実験結果に基づいた本手法の有効性について考察する．最後に，6 章でまとめと今後の課題について述べる．

2. 関連研究

本稿で採用する HAZOP は，外部視点で観察可能な分析対象のパラメータに対して，多い，少ないといった正常な状態からの逸脱を導き出すガイドワードを組み合わせることでハザードを抽出する分析手法である [2]．様々な分野に適用可能な手法として有効性が確認されているが，分析結果が対策されたことの証跡との対応づけは定義していない．また，FTA は，分析対象にとって望ましくない事象を故障木と呼ばれるゴールツリーのトップイベントに設定し，分析対象の構造などに基づいてサブイベントに分解することで，その事象を引き起こす分析対象の内部要因を特定する手法である [3]．サブイベントへの分解には，AND 分解，OR 分解を用いることができ，分解されたサブイベント間の関係性を表現することが可能である．ただし，HAZOP 同様に分析結果の対策に関する証跡との対応づけは定義していない．D-Case は，GSN（Goal Structuring Notation）[4], [5] を拡張した記法であり，トップゴールに記述した主張を戦略ノードの記述内容に従ってサブゴールに AND 分解し，さらにその過程で用いた基準などの情報を前提ノードで表現しながら，最下位となるサブゴールの妥当性を証跡と関連づけたエビデンスノードで説明する，という流れでゴールツリー形式の安全性ケースを記述する．また，システム運用時の状況変化に対応することを想定したモニタノードなどを有している点が特徴である．そ

表 1 比較表：HAZOP，FTA，D-Case
Table 1 Comparison table for HAZOP, FTA, D-Case.

名称	利用工程	視点	証跡との対応づけ
HAZOP	分析	外部	不可
FTA	分析	内部	不可
D-Case	確認	外部	可

の他，ノードの接続関係の自由度が高い GSN の表記規則を部分的に制約することで，第三者の誤解釈を避ける規則が実装されている [6], [7], [8]．**表 1** に上述した HAZOP，FTA，D-Case の比較表を示しておく．

分析手法である HAZOP，FTA との組合せに関する研究としては，文献 [9], [10], [11] がある．これらの文献では安全分析における HAZOP，FTA の位置付けと他手法との組合せについて述べているが，D-Case との関係については述べていない．一方，D-Case との組合せについては，文献 [12] で HAZOP との関係を述べている．この手法では，シーケンス図に基づく D-Case の作成法を提案し，物品購入のシーケンス図に対して HAZOP によるリスク分析に基づいて D-Case が作成できることを明らかにしている．しかし，FTA との関係については考慮していないので，システムのアーキテクチャに対する内部リスクを考慮できていない点と，対策の網羅性についての確認が十分でない点に課題がある．文献 [13], [14] で FTA を証拠に用いた D-Case の構造が示されているが，具体的な FTA の分析結果との組合せについては述べられていない．さらに，文献 [15] では規格化されている知識モデル群との組合せ，文献 [16] では SysML をはじめとする設計手法との組合せが述べられているが，HAZOP，FTA との関係については述べていない．

安全分析結果に基づいて D-Case を作成する手法に関する研究としては，説明構造 [17], [18], [19], [20] や説明の分解 [21], [22] に焦点を当てたパターンについて研究されているが，D-Case の作成方法については述べられていない．文献 [23], [24] では D-Case の作成手順に関して述べているが，HAZOP，FTA との関係は述べていない．また，文献 [25] においてモデル情報に基づいた D-Case の統一的な作成方法が提案されているが，HAZOP，FTA の分析結果を事例とした適用評価は行われていない．

車載ソフトウェア業界が必要とする安全分析環境としては，システムの利用者が期待する正常な動作の逸脱状態をハザードとして抽出し，その発生につながるシステム内部の要因の特定と対策を立案し，さらにその過程の妥当性と対策状況を第三者に説明できる必要がある．上記課題は，HAZOP，FTA，D-Case の組合せで解決が期待できるが，HAZOP，FTA を用いた分析時にどのような情報の記録が必要で，D-Case においてどのように利用されるべきかが明らかにされていない．本稿では，上述した 3 つの手法の

組み合わせ方について次章以降で説明していく．

3. D-Case を導入した安全分析手法

3.1 研究仮説

車載システムに対する安全分析の結果を分析作業の当事者ではない第三者が納得するためには，安全分析を支える工程間の関係，およびそれぞれの工程の分析過程が妥当であり，さらに導出された結果がシステムに対して確実に反映されていることを確認できる必要がある．このために可視化すべき情報としては以下があげられる．

- 工程ごとの分析結果の関係を示した全体像の情報
- 網羅的な分析結果を導くために用いた判断の情報
- システムに対する分析結果の実施状況の情報

従来から安全分析で利用されている HAZOP，FTA では，分析の網羅性の根拠を示すことができないため，分析者の用いた知識が暗黙知化し，第三者が確認できないという問題があった．また，それぞれの分析結果の関係を可視化し，安全分析全体を確認する記法，および分析結果がシステムに対して実施されたことの証跡を確認する記法も提供していない．このため，従来の手法では，HAZOP，FTA だけでは不足する上記情報を可視化するために，自由記述の自然言語文章を作成することで補っている．しかしながら，自由記述された文章は，分析結果を段階的に説明する過程で網羅性に不備が生じるなど，作成者のスキルによって記述品質が大きく変動するため，不足する情報が必ずしも正しく補えるとは限らない．

本稿では，HAZOP，FTA に D-Case を組み合わせることで，上述した課題を解決する手法を 3.2 節で提案する．D-Case は，抽象度の高い主張を明文化された客観的な記述に基づいて網羅的に分解して具体化する記法であり，主張の特性や主張の妥当性を証明する根拠についても可視化が求められる．この制約に従って安全分析結果の説明内容を記述することで，自由記述の自然言語文章と比べて，説明内容の網羅性や客観性に関して安定した記述品質が期待できる．ただし，D-Case だけでは根拠の選択などに自由度が高く，現場運用するには限界がある．このため，本稿が提案するように，安全分析における利用手順が明文化された HAZOP，FTA と組み合わせることで，この課題の解消も期待できる．

なお，従来手法と提案手法の相違点を**表 2** に示す．分析工程ではどちらも HAZOP，FTA が採用されているが，従来手法では HAZOP，FTA の利用手順が現場の分析者に依存しており，確認工程で必要となる情報が HAZOP，FTA を用いた分析工程で考慮されていない可能性がある．一方，提案手法では，D-Case 作成時に必要となる情報が明文化されており，HAZOP，FTA，対策確認表の作成過程で必要な情報を確実に記録することができる．

上述した従来手法の問題点が提案手法によって解決できることを，以下の研究仮説として設定し，5 章で研究仮説の達成状況を実験結果に基づいて確認する．

- 研究仮説 1：提案手法が従来手法よりも，安全分析全体を確認するうえで有効である．
- 研究仮説 2：提案手法が従来手法よりも，分析過程で用いた判断根拠を確認するうえで有効である．
- 研究仮説 3：提案手法が従来手法よりも，ハザード対策の組み込み状況を確認するうえで有効である．
- 研究仮説 4：提案手法は，D-Case の記述品質に関する問題を解消するうえで有効である．

表 2 安全分析工程と採用手法
Table 2 Safety analysis process and adapted method.

工程	従来手法	提案手法
利用者視点でのハザード抽出（外部分析）	HAZOP	HAZOP
開発者視点でのハザード要因の抽出（内部分析）	FTA	FTA
開発者視点での対策確認（内部確認）	自然言語文章（自由記述）	対策確認表
利用者視点での対策確認（外部確認）	自然言語文章（自由記述）	D-Case

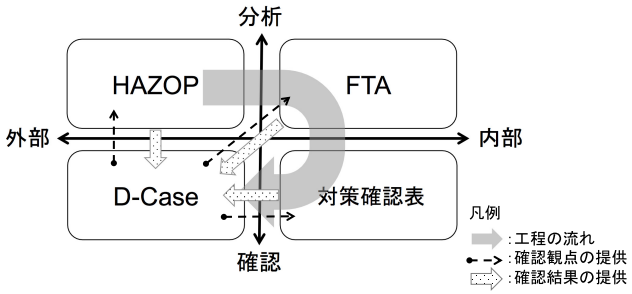

図 1 提案手法の構成
Fig. 1 The configuration of proposed method.

3.2 提案手法

第三者への説明責任が求められる ISO26262 への対応を想定した安全分析では，1 章で述べた 4 つの工程とそれぞれの工程で用いる手法の標準化が不可欠となる．本節では，それぞれの工程に対して表 2 の提案手法を割り当てた**図 1** に示す安全分析手法の構成と分析手順について説明する．本提案は，安全分析工程を「分析と確認」，「外部と内部」の視点で分割したうえで，それぞれの工程の特性に合わせて最適な手法を割り当てている．このように，「分析と確認」，「外部と内部」という 2 つの視点で，HAZOP，FTA，対策確認表，D-Case を組み合わせた統合手法が本提案の特徴である．各工程の詳細について次節以降で説明する．

3.2.1 利用者視点でのハザード抽出

本工程では，安全分析の対象となるシステムが外部環境に及ぼす可能性のあるハザードを抽出する．ハザードはシ

ステムと外部環境の間に位置するパラメータの逸脱状態として抽出する．具体的な手順を以下に記す．

(1) システムと外部環境の間に存在するパラメータを明らかにする．
(2) HAZOP 分析に用いるガイドワードを IEC61882 の定義から選定する（ない，多い，少ないなど）[26], [27]．
(3) パラメータとガイドワードの組合せからパラメータの逸脱状態を抽出する．

3.2.2 開発者視点でのハザード要因の抽出

本工程では，3.2.1 項で抽出したハザードを引き起こす要因を抽出する．ハザードを引き起こす要因は，FTA を用いて以下の手順で抽出する．

(1) FTA のトップイベントに 3.2.1 項で抽出したハザードを設定する．
(2) 安全分析の対象となるシステムに関する設計情報（システム構成など）に基づいてサブイベントに分解する．
(3) 分解に用いる設計情報がなくなるまで分解を繰り返す．
(4) 最下位のサブイベントに対して想定される故障モード要因を明らかにする．
(5) 最下位のサブイベントと故障モード要因の組合せからハザード要因を明らかにする．

3.2.3 開発者視点での対策確認

本工程では，3.2.2 項で抽出したハザード要因を解決するための対策を定義する．対策は与えられている設計情報に基づき，その要因と関連づけられているハードウェア，ソフトウェアを明らかにしたうえで，最適な箇所での実装方法を表形式でまとめる（本表を対策確認表と呼ぶ）．

3.2.4 利用者視点での対策確認

3.2.3 項までの工程で作成した分析結果に基づき，第三者への説明に用いる安全性ケースを D-Case 形式で作成する．

(1) トップゴールに「対象となるシステムは安全である」を設定する．
(2) トップゴールの主張を 3.2.1 項で行った HAZOP 分析結果に基づいて分解する．分析結果を導出した根拠として HAZOP 分析に用いたパラメータとガイドワードを関連づける．
(3) ハザード対策の安全性を 3.2.2 項で行った FTA 分析結果に基づいてハザード要因に至るまで分解する．分解の根拠として，FTA 分析で分解に用いたシステム構成と故障モード要因を関連づける．
(4) ハザード要因への対策の安全性を 3.2.3 項で作成した対策確認表に基づいて分解する．対策箇所の網羅性の根拠として，ECU ソフトウェア構成を関連づける．
(5) 最下位のゴールに記された対策内容が実際のシステムに組み込まれていることを確認できる証拠を紐づける．

4. 手法の適用実験

本章では，被験者に与えた情報の形式の差が理解に与える影響を比較するために，従来手法，提案手法それぞれを用いて作成した安全性ケースの比較実験について述べる．

表 3 機能一覧
Table 3 Function list.

ID	機能
1	ユーザの ON 操作でヘッドライトを点灯する
2	ユーザの OFF 操作でヘッドライトを消灯する

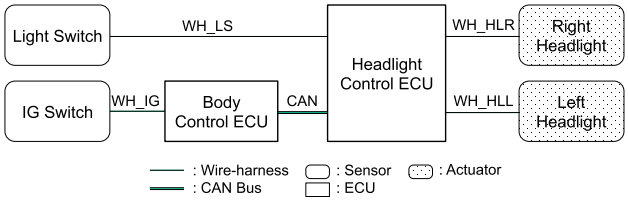

図 2 システム構成
Fig. 2 System structure.

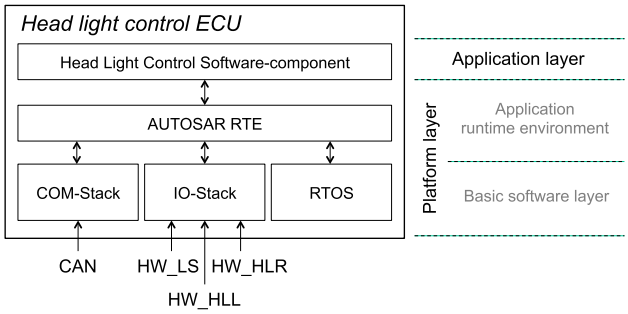

図 3 ECU ソフトウェア構成
Fig. 3 ECU software structure.

4.1 実験対象

本節では，実験対象となるヘッドライト制御システムについて定義する．本実験においては，本節で記した設計情報の範囲に対して安全分析を実施したことを注意しておく．

4.1.1 ヘッドライト制御システム

ヘッドライト制御システムが提供する機能を**表 3** に示す．また，ヘッドライト制御システムの構成を**図 2** に示す．図中の凡例に示されているとおり，ヘッドライト制御システムは大きく分けてセンサ，ECU（Electronic Control Unit の略称），アクチュエータの 3 分類で構成されており，外界の情報をセンサで読み取り，その情報に基づいて ECU がアクチュエータの制御方法を計算し，その結果に従ってアクチュエータが外界に作用する，という流れで前述の機能が実現される．本システムの前提条件として，センサ，アクチュエータは故障することはないものとする．

4.1.2 ヘッドライト制御 ECU ソフトウェア

図 3 にヘッドライト制御 ECU のソフトウェア構成を示す．ボデー制御 ECU もアプリケーション層のコンポーネントが異なるのみで同様の構成を有するものとする．なお，

本実験では，システムレベルの安全分析に焦点を置くため，ECU のハードウェア構成要素の定義は省略し，ハザード対策を組み込むソフトウェア構成要素のみ定義する．

表 4 質問内容
Table 4 Question list.

ID	質問内容
Q1	HAZOP 分析の対象となるパラメータを抽出する際に用いた設計情報の記述箇所を述べよ．
Q2	HAZOP 分析のガードワードを選定する際に用いた設計情報の記述箇所を述べよ．
Q3	FTA 分析のトップイベントの分解が ECU に対してのみ行われている理由の記述箇所を述べよ．
Q4	FTA 分析の最下位イベントに相当するハザード要因を抽出する際に用いた設計情報の記述箇所を述べよ．
Q5	ハザード要因への対策箇所を特定する際に用いた設計情報の記述箇所を述べよ．

4.2 実験内容

比較対象となる安全性ケースは，ともに HAZOP，FTA，D-Case を利用した経験のある同一のエンジニアが作成し

表 5 HAZOP 分析結果
Table 5 HAZOP analysis result.

ID	Parameter	Guideword	Hazard
1	Light intensity	No	Total loss of headlight
2		More	More light intensity
3		Less	Less light intensity

表 6 故障モード要因
Table 6 Generic failure mode.

Structural element	Generic failure mode
Wire-harness	disconnect
	noise effect
ECU	failure

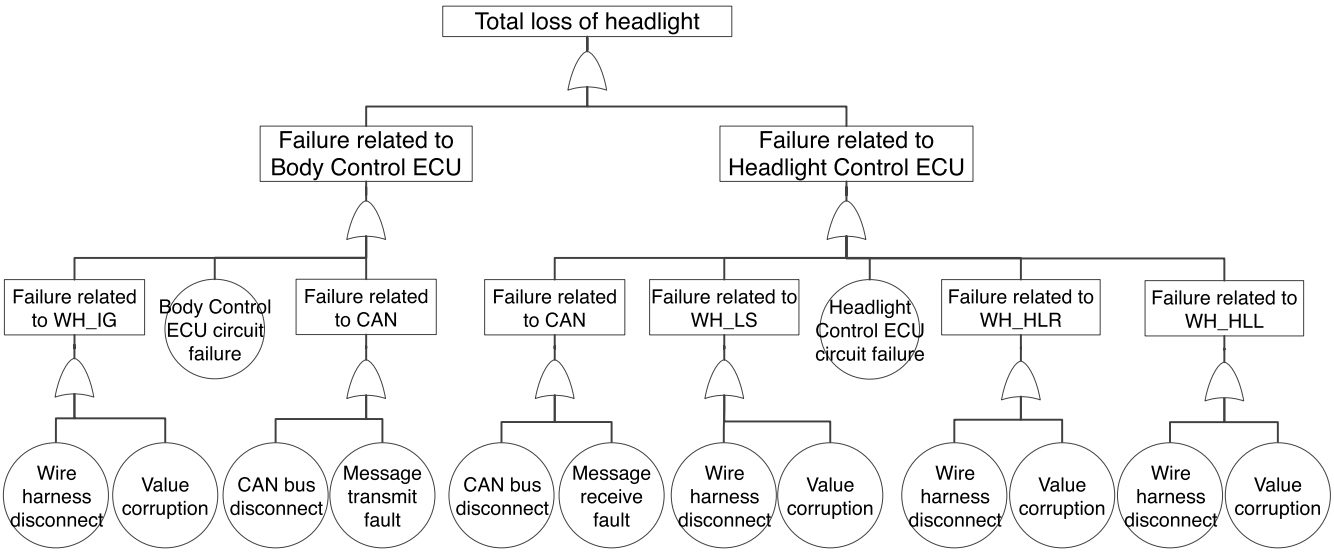

図 4 FTA 分析結果
Fig. 4 FTA analysis result.

表 7 対策確認表
Table 7 Countermeasure confirmation table.

ID	Device	Failure mode	Countermeasure
1	Body	WH_IG: Wire harness disconnect	Circuit sets ON to IG Switch value
2	Control	WH_IG: Value corruption	IO-Stack provides preventing the chattering
3	ECU	Body Control ECU hardware breakdown	Headlight Control ECU monitors and adresses
4		CAN: CAN bus disconnect	Same as above
5		CAN: Message transmission fault	Same as above
6	Headlight	CAN: CAN bus disconnect	COM-Stack sets ON to IG Switch value
7	Control	CAN: Message receive fault	Same as above
8	ECU	WH_LS: Wire harness disconnect	IO-Stack sets ON to Light Switch value
9		WH_LS Value corruption	IO-Stack provides preventing the chattering
10		Headlight Control ECU hardware breakdown	Body Control ECU monitors and indicates the caution
11		WH_HLR: Wire harness disconnect	Circuit addresses in Right Headlight
12		WH_HLR: Value corruption	Circuit provides preventing the chattering in Right Headlight
13		WH_HLL: Wire harness disconnect	Circuit addresses in Left Headlight
14		WH_HLL: Value corruption	Circuit provides preventing the chattering in Left Headlight

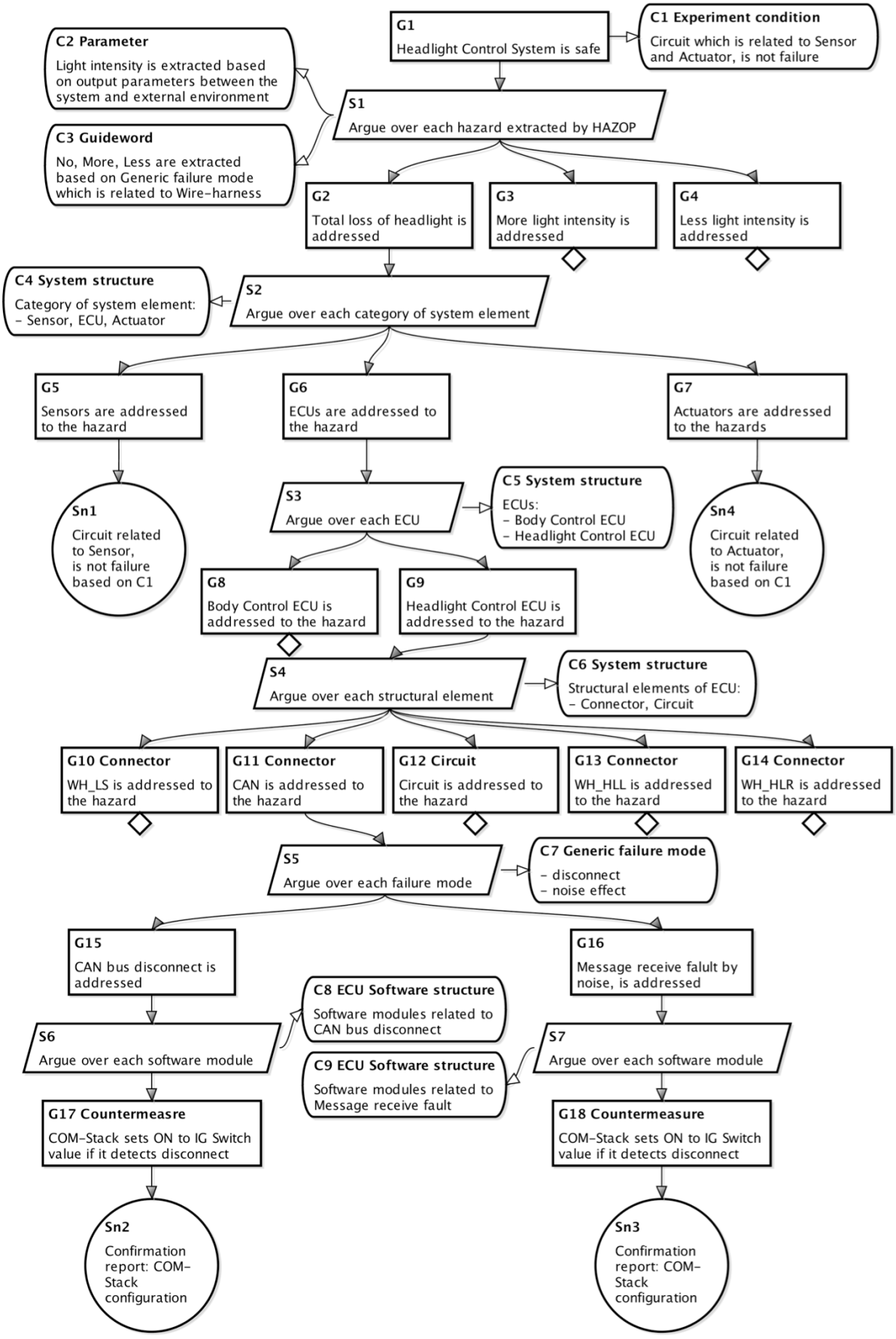

図 5 D-Case を用いた安全性ケース
Fig. 5 Safety case using D-Case.

た結果であり，従来手法が 4.3 節の全文，提案手法が図 5 に対応する．従来手法における開発者視点での対策確認（内部確認）の結果は，表 2 に示したとおり自然言語文書となるが，本実験では被験者が FTA の分析結果との対応づけを確認しやすくするために，対策確認表を採用している．実験手順としては，第三者が安全性ケースの妥当性を判断する際に，その根拠として確認が必要となる内容を**表 4** に示す質問形式とし，その回答時間と正答率を計測する．なお，3 年以上のソフトウェア開発経験を有した技術者を対象として，従来手法を先に実施するグループ（被験者 A1～A5）と提案手法を先に実施するグループ（被験者 B1～B5）に分けて実験を行う．

4.3 従来手法を用いた安全性ケース

本節では，ヘッドライト制御システムの安全性分析結果を説明する．システムの詳細は 4.1 節を参照されたい．

4.3.1 ハザード抽出

本実験では，HAZOP 分析の対象とするパラメータとして，システムと外部環境（他車，歩行者など）の間に存在するパラメータであるヘッドライトの光量を採用する．また，ガイドワードには No，More，Less を選定した．上記 2 つの判断結果と，その組合せに基づいて抽出されたハザード一覧の記録を**表 5** に示す．なお，本稿では ID.1 のみを対象として以降の実験を進める．

4.3.2 ハザード要因の抽出

4.3.1 項で抽出した ID.1 のハザード「Total loss of headlight」が設定されたトップイベントを図 2 のシステム構成で定義された設計情報に従って分解した．そのうえで最下位のイベントに対して，**表 6** に示した故障モード要因を組み合わせることで末端の基本イベントとしてハザード要因を抽出した（**図 4** 参照）．

なお，実際の開発現場では，故障モード要因には分析時の知見として資産化されているものが再利用されるが，本実験では簡易化のため表 6 の内容にとどめている．

4.3.3 対策確認

4.3.2 項で導き出したハザード要因を解消するための対策を**表 7** に示す表形式に従って定義した．

4.4 提案手法を用いた安全性ケース

提案手法を用いた安全性ケースを**図 5** に示す．トップゴールは安全分析の手順に沿って以下の順で分解している．文中のラベルは図 5 のノードラベルに対応している．

(1) HAZOP 分析の結果に基づきトップゴールを分解（G2, G3, G4）．

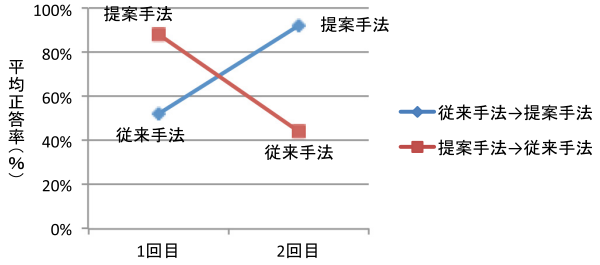

図 6 従来手法と提案手法の比較：正答率
Fig. 6 The summary of comparison result: correct rate.

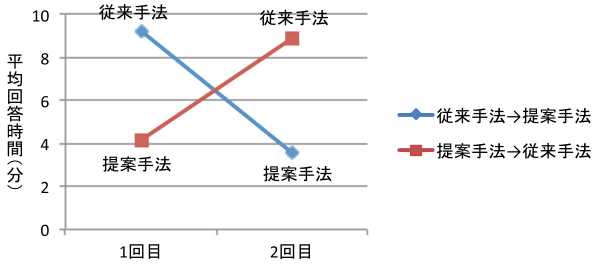

図 7 従来手法と提案手法の比較：回答時間
Fig. 7 The summary of comparison result: response time.

表 8 従来手法と提案手法の比較結果
Table 8 The Comparison result.

被験者		従来手法							提案手法						
		回答時間	正答率	正答率内訳 Q1	Q2	Q3	Q4	Q5	回答時間	正答率	正答率内訳 Q1	Q2	Q3	Q4	Q5
従来手法→提案手法	A1	8m30s	40%	○	×	×	○	×	4m25s	80%	○	○	×	○	○
	A2	16m00s	60%	○	×	○	×	○	4m44s	100%	○	○	○	○	○
	A3	4m00s	60%	○	×	○	○	×	1m28s	100%	○	○	○	○	○
	A4	7m30s	60%	○	×	○	○	×	4m00s	80%	○	○	○	○	×
	A5	10m00s	40%	×	×	○	○	×	3m00s	100%	○	○	○	○	○
	平均	9m12s	52%	80%	0%	80%	80%	20%	3m30s	92%	100%	100%	80%	100%	80%
提案手法→従来手法	B1	13m30s	40%	○	×	○	×	×	5m20s	100%	○	○	○	○	○
	B2	5m00s	40%	×	×	○	○	×	2m00s	100%	○	○	○	○	○
	B3	7m30s	60%	○	×	○	×	○	4m30s	80%	○	○	○	○	×
	B4	8m00s	40%	○	×	○	×	×	4m00s	80%	○	○	○	×	○
	B5	10m10s	40%	○	×	○	×	×	5m00s	80%	○	○	○	×	○
	平均	8m48s	44%	80%	0%	100%	20%	20%	4m12s	88%	100%	100%	100%	60%	80%

(2) システム構成：機器分類（センサ，ECU，アクチュエータ）に基づき分解（G5，G6，G7）．
(3) システム構成：機器（ボデー制御 ECU，ヘッドライト制御 ECU）に基づき分解（G8，G9）．
(4) システム構成：機器の構成要素（コネクタ，電気回路）に基づき分解（G10，G11，G12，G13，G14）．
(5) 故障モード要因（ハーネス：断線，ノイズ，電気回路：故障）に基づき分解（G15，G16）．
(6) ECU ソフトウェア構成に基づき分解（故障モードに関連するソフトウェアモジュールのみ）（G17，G18）．

なお，本稿ではヘッドライト制御 ECU の CAN bus に関する対策の説明のみすべて掲載し，それ以外は省略している（該当箇所は D-Case の Undeveloped に相当）．

4.5 実験結果

4.2 節に従って比較実験を行った結果を**図 6**，**図 7** に示す．結果詳細は**表 8** を参照されたい．

5. 考察

5.1 研究仮説 1 の実証

従来手法では，HAZOP，FTA それぞれ単独での利用方法は定義されていたが，その分析結果の統合手順は定められておらず，自由記述の自然言語で安全性ケースを記述する分析者に依存した記述品質となっていた．一方，提案手法では，HAZOP，FTA の分析結果だけでなく，その分析過程で用いられた判断基準を含めて D-Case 上で可視化すべき情報を明らかにし，それらの情報の統合方法を D-Case の作成手順として定義している．この結果，それぞれの分析工程が適切に履行されていることの確認を含めて，安全分析全体を示すことが可能となる．また，本手法を用いることで，分析に用いた手順や判断基準が明文化できるため，それらを再利用可能な知識として蓄積する効果も期待できる．**表 9** に示した被験者の意見からも，説明の流れや構造が可視化され（O1，O2），かつ説明の単位も適切に部品化されたことで（O3，O4），従来手法と比べて理解が容易になっていることが分かる．本結果から研究仮説 1 は実証できたといえる．

5.2 研究仮説 2 の実証

HAZOP，FTA の分析過程で用いた判断の根拠は，従来手法では自由記述の自然言語文章として記録されるため，文章の品質によっては記述箇所の特定が困難となる場合が発生する．このため，第三者の理解に要するコストが高くなってしまう．一方，本稿で提案した D-Case を安全性ケースに用いた場合，前提ノードで示した判断の根拠が確認の過程で適切に紐づけられて確認できる．

4.5 節の実験結果においても，従来手法の正答率が 50%程度であることに対して，本提案の正答率は 90%前後を得ている．従来手法の質問 Q2，Q5 の正答率が低い原因を被験者に確認したところ，分析結果の記述箇所から該当する記述箇所を参照する記述が明文化されておらず，分析結果から分析者の意図を類推して該当箇所を探す必要があるためであった．一方，提案手法で不正解のあった質問 Q3 について被験者に確認したところ，該当箇所である C1 への参照関係がノード Sn1，Sn2 の文中に記述されており，そこまで踏み込んで確認できなかったことが原因であった．また，質問 Q4，Q5 は，ハザード要因という用語が D-Case 上で明記されていないため，該当箇所を誤解釈したことが原因であった．なお，従来手法と提案手法の実施順序によらず，提案手法の正答率が高かった理由としては，表 9 の被験者の意見にもあげられているとおり，質問に対する関連箇所を絞り込むことが容易であり，さらに D-Case の記法上，分析時に用いた判断に関する記述は前提ノードに記されていることが明白であるため，その特定が容易であったことがあげられる．回答時間についても従来手法と比べて半分以下の時間で確認できており，研究仮説 2 は実証できたといえる．なお，回答時間の短縮は，表 9 の O5 にあがっているように，質問内容の回答となる判断の根拠が前提ノードに集約して表現されていた効果と予想される．また，O1 にあがっているように，D-Case は分析結果の説明が上から順に構造化されるため，質問の関連箇所の特定が容易であったことも一因と予想される．

表 9 D-Case に対する被験者の意見
Table 9 The Opinions of experimenters for D-Case.

ID	被験者の意見
O1	上から順に読めば分析結果を順序立てて理解できるのが良い
O2	確認時に注目する必要のある領域が絞られるので読みやすい
O3	説明が適切に部品化されるため全体理解が容易である
O4	ノード内の文章が長文でないので理解しやすい
O5	判断の根拠が前提ノードにまとまっているので見つけやすい

5.3 研究仮説 3 の実証

実験結果の図 4 が示すように，研究仮説 3 で設定したハザード対策の組み込み状況の確認は，FTA だけでは表現できない．これに対して D-Case では，最下層のゴールノードで対策を記し，その対策が組み込まれていることの確認記録を記した証拠ノードと紐づけることで，組み込み状況を可視化できている（図 5 の G17 と Sn2，および G18 と Sn3 の関係に相当）．上記結果から，本稿の提案手法は研究仮説 3 を実証できたといえる．

5.4 研究仮説 4 の実証

D-Case の記述品質は作成者のスキルによって左右されることが分かっている [28]．この問題は，D-Case の十分な作成手順が提示されていないことに原因があり，たとえ

ば，HAZOP，FTA を D-Case のエビデンスに用いる，という曖昧な手順しか提示されていなかった．このため，安全分析に D-Case だけを導入しても，外部視点でのハザード抽出や内部視点でのハザード要因の抽出手順が不明確な D-Case を作成する可能性が高く，開発現場での運用が困難であった．提案手法では，HAZOP，FTA を用いた分析工程の手順を定義し，その過程で用いた判断基準に基づいて D-Case を作成する手順を提案している．提案手法に従って作成した D-Case は，表 8 に示したとおり，90%前後の正答率を得ており，高い記述品質を保つことができている．この結果から，本稿の提案手法は研究仮説 4 を実証できたといえる．

5.5 本稿の限界

本手法の有効性は，本稿で示した事例のみに基づいて評価しており，複数の事例に基づいた統計的な検証はしていない．対象となるシステムの規模や複雑さといった条件の異なる複数の事例に適用し，本稿と同様の効果が得られることを確認する必要がある．また，本稿では作成した安全性ケースに関する理解度の実験のみを行っており，作成効率に関する従来手法との比較が必要である．

6. 結論

本稿では，「分析と確認」ならびに「外部と内部」の視点で HAZOP，FTA，対策確認表，および D-Case を組み合わせた安全分析手法を提案した．本手法を採用することで，第三者の確認時に不可欠となる情報を可視化したうえで安全分析結果を説明でき，さらに，簡易的なヘッドライト制御システムへの適用事例に基づいて，その有効性を確認した．また，本稿で採用した HAZOP，FTA，D-Case は，それぞれ単独では課題をかかえていたが，それらを緊密に組み合わせることで互いの課題の解消を図り，第三者が正しく理解できる安全性ケースの作成手順を確立することができた．今後の課題として，実際の車載システムへの適用事例を増やし，その結果に基づいて本手法の有効性を統計的に検証していく必要がある．さらに，HAZOP や FTA の分析結果を準形式化し，その記述規約に基づいて D-Case を自動生成する仕組みについて考案していく予定である．本仕組みが実現されれば，エンジニアは自身の分析結果を第三者の視点で確認することが可能となる．

参考文献

[1] 独立行政法人情報処理推進機構：セーフティ設計・セキュリティ設計に関する実態調査結果，独立行政法人情報処理推進機構 (2015).

[2] Dunjó, J., Fthenakis, V., Vílchez, J.A. and Arnaldos, J.: Hazard and operability (HAZOP) analysis, A literature review, *Journal of hazardous materials* (2010).

[3] de Queiroz Souza, R. and Álvares, A.J.: FMEA and FTA analysis for application of the reliability-centered maintenance methodology: Case study on hydraulic turbines, *ABCM Symposium Series in Mechatronics* (2008).

[4] Kelly, T. and Weaver, R.: The goal structuring notation–a safety argument notation, *Proc. dependable systems and networks 2004 workshop on assurance cases* (2004).

[5] Attwood, K., Chinneck, P., Clarke, M., Cleland, G., Coates, M., Cockram, T. and Williams, P.: GSN Community Standard Version 1, Technical Report, GSN Working Group (2011).

[6] Tokoro, M.: *Open Systems Dependability*, CRC Press (2015).

[7] 高井利憲，山本修一郎，松野　裕：D-Case 入門ディペンダビリティ・ケースを書いてみよう!，株式会社ダイテックホールディング (2012).

[8] 松野　裕, 山本修一郎：実践 D-Case ディペンダビリティ・ケースを活用しよう!，株式会社ダイテックホールディング (2013).

[9] Allenby, K. and Kelly, T.: Deriving safety requirements using scenarios, *5th IEEE International Symposium on Requirements Engineering*, IEEE, pp.228–235 (2001).

[10] Dimitrakos, T., Ritchie, B., Raptis, D. and Stølen, K.: Model-based security risk analysis for Web applications: The CORAS approach, *Proc. EuroWeb* (2002).

[11] Fenelon, P. and Hebbron, B.: Applying HAZOP to software engineering models, *Risk Management And Critical Protective Systems: Proc. SARSS* (1994).

[12] Ding, F., Yamamoto, S. and Abrahim, N.: The Method of D-Case Development Using HAZOP Analysis on UML Models, *JCKBSE, Communications in Computer and Information Science*, pp.631–644 (2014).

[13] Matsuno, Y. and Taguchi, K.: Parameterised Argument Structure for GSN Patterns, *2011 11th International Conference on Quality Software* (*QSIC*), IEEE, pp.96–101 (2011).

[14] Matsuno, Y. and Yamamoto, S.: A Framework for Dependability Consensus Building and In-Operation Assurance, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, pp.1–17 (2013).

[15] Yamamoto, S.: A Knowledge Integration Approach of Safety-critical Software Development and Operation based on the Method Architecture, *Procedia – Procedia Computer Science*, pp.1718–1727, Elsevier Masson SAS (2014).

[16] Habli, I., Ibarra, I., Rivett, R.S. and Kelly, T.: Model-Based Assurance for Justifying Automotive Functional Safety, *Proc. 2010 SAE World Congress*, SAE International (2010).

[17] Hawkins, R. and Kelly, T.: *A software safety argument pattern catalogue*, The University of York (2013).

[18] Alexander, R., Kelly, T., Kurd, Z. and McDermid, J.A.: *Safety cases for advanced control software: Safety case patterns* (2007).

[19] Kelly, T. and McDermid, J.A.: Safety Case Construction and Reuse Using Patterns, *Safe Comp 97*, pp.55–69, Springer London, London (1997).

[20] Kelly, T.: Arguing safety: A systematic approach to managing safety cases, Ph.D. Thesis, University of York (1999).

[21] Bloomfield, R. and Bishop, P.: Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective, *Making Systems Safer*, pp.51–67, Springer London, London (2010).

[22] 山本修一郎，松野　裕：ディペンダビリティケース分解

パターンについての考察，電子情報通信学会技術研究報告 (2013).
[23] Palin, R. and Habli, I.: *Assurance of automotive safety – A safety case approach* (2010).
[24] Patu, V. and Yamamoto, S.: How to develop Security Case by combining real life security experiences (evidence) with D-Case, *Procedia Computer Science*, pp.954–959 (2013).
[25] Yamamoto, S., Morisaki, S. and Atsumi, N.: A unified approach on assurance case development method based on models, *SIG-KSN* (2015).
[26] International Electrotechnical Commission: *IEC 61882: Hazard and operability studies* (*HAZOP studies*) – *Application guide*, International Electrotechnical Commission (2001).
[27] Pumfrey, D.J.: The principled design of computer system safety analyses, Ph.D. Thesis, University of York (1999).
[28] Yamamoto, S., Morisaki, S., Atsumi, N., Kondo, J. and Oobayashi, H.: An experimental evaluation of GSN review, *SIG-KSN* (2016).

小林 展英 （学生会員）

1997 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．同年（株）デンソークリエイト入社．2015 年より名古屋大学大学院情報科学研究科博士後期課程在籍．電子情報通信学会，人工知能学会各会員．

森崎 修司 （正会員）

2001 年奈良先端科学技術大学院大学情報科学研究科博士課程修了．2013 年 10 月より名古屋大学大学院情報科学研究科准教授．博士（工学）．ソフトウェアレビュー，実証的ソフトウェア工学の研究に従事．IEEE，電子情報通信学会，プロジェクトマネジメント学会各会員．

山本 修一郎 （正会員）

1979 年名古屋大学大学院工学研究科情報工学専攻修了．同年日本電信電話公社入社．2016 年 4 月より名古屋大学大学院情報科学研究科教授．ソフトウェア工学，要求工学，エンタープライズアーキテクチャの研究に従事．博士（工学）．電子情報通信学会，人工知能学会，プロジェクトマネジメント学会，ACM，IEEE 各会員．