論文審査の結果の要旨

氏名：越　山　　勉
博士の専攻分野の名称：博士（工学）
論文題名：記述者視点に基づくGSNのパターン分類によるセーフティケース記述の容易化に関する研究
審査委員：　（主査）　教授　高　橋　　聖
　　（副査）　教授　細　野　裕　行　　准教授　松　野　　裕
　　特任教授　泉　　隆

本論文の研究領域は，自動車などの開発におけるシステムの安全性保証である。近年欧米において，システムの安全性保証に関する手法として，単なるチェックリストだけではなく，その安全性がなぜ達成されているか，議論を構築し，テスト結果などのエビデンスにより示す「セーフティケース(Safety Case)」の考え方が重要視されてきている。日本においても自動運転も含む自動車の機能安全分野においてセーフティケースが国際規格適合の面からも必要になりつつある。しかしながらセーフティケースをどのように記述すればよいのか，具体的な手法やサンプルがほとんどなく，特に日本においてセーフティケースは普及していない。申請者は自動車会社に勤務しており，機能安全に関する職務の中で，セーフティケースの重要性を認識し，社内でのセーフティケースの普及を検討してきた。セーフティケースの記述手法であるGSN(Goal Structuring Notation)に着目し，GSNを記述者の視点からパターン化することにより，セーフティケースの記述を容易化できるのではないかと洞察し，博士後期課程に入学しGSNモデルのパターン化に関する研究を以下のようにまとめた。

提出論文は，第1章の序論から第8章の結論に至る全8章から構成されている。

「第1章 序論」では，本研究の背景と目的，本論文の構成および用語の定義について説明されている。本章では，GSNモデルを用いたセーフティケース記述の容易化という本研究の課題を明確に浮き上がらせており，本論文の重要性が明確になっている点で評価できる。

「第2章 GSNの基本構造について」では本研究で用いるセーフティケースの表記法であるGSN(Goal Structuring Notation)の基本構造について説明している。GSNは基本的にゴール，ストラテジ，コンテキスト，エビデンスという4種類のノードを用いて記述されるが，これらのノードをわかりやすく説明している。本研究ではストラテジの働きに注目し，従来のゴール分割に加えてゴールを変換する役割があることを見出し，ゴール分割と変換によりGSNモデルを記述者の視点からパターン化できることを示した。GSNの基本を説明しつつ，従来にないGSNモデルのパターン化を導入していることは評価できる。

「第3章 GSNのパターン分類」では第2章に基づき記述者の視点からGSNモデルを6種類のパターンに分類している。従来のセーフティケースのパターン化の研究では，自動車や原子力発電所などのシステムの領域ごとの具体的なパターンや，FTA(故障木解析)におけるトップ事象の分割を参考にした機能やシステムの構成に基づくパターンが提案されてきた。本研究では記述者がゴールをどのような視点で分割するかを少数のGSNモデルをもとに検討し，以下のように分類分けをしている：(a)部分選択，(b)二重否定，(c)基準化，(d)視点変換，(e)合わせ技，(f)MECE(Mutually Exclusive, Collectively Exhaustiveの略)。これらのパターンの特徴は，従来のGSNパターンと異なり記述者がゴールを論理的に分割している((a)，(b)，(c)，(f))のか，そうでない((d)，(e))のかによりパターン化していることであり，さらにそれぞれの分割がゴールの主張を弱めているのか，等価のままなのか，あるいは強めているか，強いとも弱いとも言えないのかにより6パターンに場合分けしている。セーフティケースのパターン化は高安全性が要求される分野，特に機能安全分野において20年以上活発に研究されている分野であり，その分野において新規性のあるパターンを提案していることは評価できる。

「第 4 章 GSN のパターンマッチング」では，公開されている GSN モデルをできるだけ収集し，提案する 6 種類の GSN パターンが既存の GSN モデルに適合するか調査している。インターネットで公開されている GSN を用いたセーフティケース関連の論文は 1025 本であった。その内，GSN の提案者であるイギリス York 大学の Tim Kelly 名誉教授が関連している論文 89 本を抽出し，GSN モデル 271 個を調査した。その結果，717 の GSN モデルの部分すべてにおいて提案する 6 パターンのいずれかが適合した。このことは提案する 6 パターンの妥当性を示している。従来の GSN パターンに関する研究では GSN パターンの提案のみにとどまっている研究が多く，本研究のように既存の GSN モデルとの適合を示した研究は少ないことから評価できる。また，論理的でないゴール分割である(d)視点変換および(e)合わせ技がパターン適合の結果，半数以上を占めていることから，安全性論証が必ずしも論理的な議論だけではなく，安全分析の専門家や技術者の論理的に説明できない経験的な知識も含めて実施されていることが示唆され興味深いと考えられる。

「第 5 章 ワークショップによる検証」では提案する 6 種類の GSN パターンを実際に企業の技術者にワークショップ形式で紹介し，GSN モデルを記述する演習を実施することにより，提案する 6 種類の GSN パターンにより GSN モデルの記述が容易になることを実証している。ワークショップは 2 回実施され，1 回目(2020 年 12 月 22 日)はあるモデルベースツール会社内でのクローズドなワークショップとして開催，2 回目(2021 年 4 月 28 日)はインターネットで参加者を募集するオープンなワークショップとして開催し，それぞれ 11 名の参加者を得て COVID-19 の感染拡大の状況の中，両方のワークショップともオンラインで実施したことが報告されている。ワークショップの結果，セーフティケースや GSN に詳しくない参加者も，提案する 6 種類の GSN パターンを用いて GSN モデルを記述することができていることを審査委員は高く評価する。さらに本論文の研究内容が，専門家のみならず，一般のワークショップ参加者からワークショップとしても高い評価を得たことから，提案する 6 種類の GSN パターンを元にした GSN ワークショップを今後も継続することにより，日本におけるセーフティケース，さらには安全性保証の一般的な考え方を普及することに本研究内容が貢献するものと期待される。

「第 6 章 既存研究における分類と考察」では，提案する 6 種類の GSN パターンを従来研究におけるセーフティケースのパターンと比較し，考察している。その結果，既存研究は部分的に本研究の提案内容と類似，一致しているものがあり，本研究の提案内容は既存の GSN パターンを包含していることが報告されている。さらに提案する 6 種類の GSN パターンは明示的に GSN のゴール分割において主張が弱まる，あるいは論理的でない分割があることを示している。このことは従来のシステム安全性保証において厳密性，論理性が強く求められることと反する。しかしながら一般にシステムの安全性を完全に保証することは不可能であり，安全性保証の議論の中でどこかで厳密性に欠け，論理的ではない部分が必ずでてくる。本研究はそのことを GSN パターンにより明示化することにより，システムの安全性保証議論のどこが論理的ではないのか，議論として弱いのか，システムのステークホルダ間で共有し合意する必要があることを示唆している。このことは，今後より複雑化・ネットワーク化し，さらに AI という，より安全性の保証が困難な技術を組み込むこれからのシステムの安全性保証に向けて重要であると考えられる。

「第 7 章 冗長機構への適用の検証」では安全性分析で用いられるシステムモデルと GSN モデルを組み合わせ，安全性保証を実施する手法を提案している。システムモデルとして日本から提案されている SCDL(Safety Concept Description Language)という，自動車の機能安全国際規格である ISO26262 で定義されている安全コンセプトを記述するためのシステムモデル上で表現されたシステムの安全性保証のための GSN モデルの構成法を提案している。第 6 章における 1 回目のワークショップにおいて，提案する GSN 構成法を演習として実施した内容を説明している。安全性分析および保証は一般にシステムモデルを参考に実施することから，本章で提案した GSN モデル構成法は評価することができる。

「第 8 章 結論」では申請者の行った研究の成果や今後の課題を述べている。安全性保証議論の構築を支援するための GSN パターンを少数の GSN モデルをもとに 6 種類提案し，その妥当性を公開されている GSN モデルをできるだけインターネットで収集し，それらがすべて提案する 6 種類の GSN パターンのいずれかに適合することを示し，2 回実施したオンラインでのワークショップにより，セーフティケー

スおよびGSNに関して知識のない一般の技術者も，提案する6種類のGSNパターンにより容易にGSNモデルを記述できることを示し，本研究の目的を達成していることを明確に結論づけている。本研究の今後の課題として，論文だけからではなく，産業界で実際に記述されているセーフティケースの調査が挙げられている。またワークショップを継続して実施することも挙げられており，今後の本研究の産業界への展開と貢献が期待される。

本研究で提案された，GSNモデルにより記述されたセーフティケースの6種類のパターンは，特に日本において，セーフティケースおよび安全性保証の一般的な考え方の普及に貢献すると考えられる。複雑化・ネットワーク化し，AIなどの新たな技術を用いて開発運用されるこれからのシステムの安全性保証は今後ますます大きな課題になると考えられる。申請者の研究はその解決に向けた一つの基礎的な研究として評価できる。

以上のことは，本論文の提出者が自立して研究活動を行い，又はその他の高度な専門的業務に従事するに必要な能力及びその基礎となる豊かな学識を有していることを示すものである。

よって本論文は，博士（工学）の学位を授与されるに値するものと認められる。

以　上

令和３年９月１６日