

卒 業 論 文

題 目

サービスロボットの遠隔操作に対する
リスクアセスメントに関する研究

指 導 教 員

大 原 賢 一 教 授

220447701
松野 有希

令和8年1月7日

名城大学
理工学部メカトロニクス工学科

論文概要

近年, サービスロボットは人手不足や働き方の変化により, 社会での需要が高まっている. 一方, 設計段階においてリスクアセスメントが十分に考慮されていない場合, 運用時に想定外のリスクが発生して危険である. 本研究は, サービスロボットの設計時・運用時における安全性確保向上を目的として, リスクアセスメントを組み込んだ設計工程を提案する.

本研究では, 提案した設計工程を自動化レベルの異なる4つのサービスロボットのユースケースに適用し, ダイアグラムを用いて危険源及びリスクの整理を行った. その結果, 自動化レベルの違いにより発生するリスクの種類や発生要因に差異が生じることが明らかとなった. また, 設計初期段階でリスクを明確化することで, 設計上のリスク低減策や運用ルールを

まだ、

検討しやすくなることが示された. ゆえに, 本研究で提案した設計工程は, サービスロボット導入時の安全性検討を支援する有効な手法であるといえる.

目次

第1章	序論	1
1.1	研究背景	2
1.2	従来研究	2
1.3	研究目的	2
1.4	おわりに	3
第2章	提案設計工程と適用ユースケースの事前情報	4
2.1	はじめに	5
2.2	リスクアセスメントの概要	5
2.2.1	リスクアセスメントシートの概要	5
2.2.1.1	表紙	6
2.2.1.2	初期分析・評価シート	6
2.2.1.3	方策後再分析シート	7
2.2.1.4	基本仕様	7
2.2.1.5	リスク値の計算	7
2.2.2	SafeML(Safe Model Language) とは	8
2.3	ロボットシステムの設計工程	9
2.3.1	SysML(Systems Modeling Language) とは	9
2.3.1.1	ドメイン構成図	10
2.3.1.2	コンテキスト図	10
2.3.1.3	要求図	10
2.3.1.4	アクティビティ図	10
2.3.1.5	ユースケース図	10
2.3.1.6	ブロック定義図	10
2.4	自動化レベル (Level of Automation)	10
第3章	RAを組み込んだ設計工程の提案	11
3.1	はじめに	12

3.2	従来設計工程の課題	12
3.3	新規提案工程の概要	13
3.4	各工程の詳細	14
3.4.1	RA シートによるリスク同定・評価	14
3.4.2	SafeML によるリスクモデル化	14
3.4.3	安全機能を SysML に反映	15
第 4 章	適用ユースケース	16
4.1	対象ユースケースの概要	17
4.2	自動化レベルの定義	17
4.3	各 LOA のユースケース	17
第 5 章	提案工程の適用結果	18
5.1	ダイアグラム化結果	19
5.2	同定された危険源・リスク	19
5.3	設計時の注意点	19
5.4	考察	19
第 6 章	納言	20
6.1	本論文のまとめ	21
6.2	今後の課題	21
	謝辞	22

目 次

2.1	cover of RA sheet	6
2.2	analysis of RA sheet	7
2.3	reanalysis of RA sheet	7
2.4	risk calculation of RA sheet	8
2.5	SafeML Model	9
3.1	sysML	12
3.2	提案設計工程	13

表 目 次

2.1 Level of Automation	10
-----------------------------------	----

第 1 章

序論

1.1 研究背景

近年, サービスロボットは少子高齢化やパンデミックによる働き方の変化により, Fig. 1.1 のような家庭内用掃除ロボットや Fig. 1.2 のような倉庫内運搬ロボット等, 様々な職業でロボットの普及が進んでいるといえる. 社会においては多様な役割を担い始めており, 特に遠隔操作型のサービスロボットは, 介護, 物流, 接客などの幅広い応用が期待されている. 実際に遠隔操作に関する先行研究も行われており, 将来的にはマニピュレータのある遠隔操作ロボットの需要は高まると考えられる.

1.2 従来研究

遠隔操作に関する研究では, 新規 VR デバイスやソフトウェアに対応するためのシステム構築 [] や操作性向上のための UI 設計 [] 等, 操作者の負担軽減や操作の直感性向上に貢献したものが数多くある. しかし, こういったロボットを扱いやすくする研究だけでは社会実装するための安全面への配慮が不十分といえる. 安全性を確保するためにはリスクアセスメント (Risk Assessment, 以下 RA とする) が重要である.

RA とは, Jis 規格 [] や ISO 規格 [] 等の国際規格に基づく工学・安全工学のプロセスであり, リスクを完全に排除するのではなく, 許容可能な水準まで低減することを目的とした手法である. RA では体系的にリスク低減を行うリスクアセスメントシートというツールがある.

遠隔操作ロボットシステムに対して, RA を実施した研究としては, レストランの配膳ロボット [] や運搬ロボット [] を対象に RA を実施し, 安全性を検討した事例が報告されている. しかし, このような研究事例は未だ少なく, 多様なユースケースを想定した検討は十分に行われていない. その結果, 遠隔操作ロボットシステムの設計・導入時に参照可能な知見が不足し, 安全設計の考え方や実施段階が設計者個人に依存することで, 運用者が個別に適応する必要が生じ, さらに設計思想が共有されない場合には安全設計がブラックボックス化する. その結果, 運用時に安全設計の意図や制約条件が十分に理解されないまま操作が行われ, 認知負荷が増大し, ヒューマンエラーが発生する可能性があるという課題がある.

1.3 研究目的

そこで本研究では, 遠隔操作のサービスロボットを対象に, 包括的なユースケースのもと, 個別事象ごとのリスクを整理し, 設計工程における安全設計プロセスを体系的に示すことを目的とする. また, 包括的なユースケースにリスクアセスメントを実施することで

ロボット導入時に活用可能な知見やテンプレートの創出を目指す。以下に、本研究のアプローチを示す。

1. 既存の設計工程 (SysML を参考とした工程) に RA の工程を組み込んだ新たな設計工程の提案
2. 自動化レベルごとに分類した 4 つのロボットユースケースに対する提案工程の適用

1.4 おわりに

本章では、本研究を行う上での背景と課題を示した。新たな安全設計プロセスを体系的に示すために、RA を組み込んだ新たな設計工程を示す。

第 2 章

提案設計工程と適用ユースケースの事前 情報

2.1 はじめに

本章では, 本研究で使用する RA, SysML, 自動化レベルについて説明する. また, 従来のロボットシステムの設計工程および従来の RA 手法を整理し, 本研究の位置づけを確認する.

2.2 リスクアセスメントの概要

リスクアセスメント [1] とは, JIS 規格や ISO 規格に基づき, 機械類に存在する危険源を体系的に洗い出し, それらによって生じるリスクを評価・低減するための規定である. RA の目的は, リスクを完全に排除することではなく, 許容可能な水準まで低減することで安全性を確保する点にある. RA は,

1. リスクシナリオの特定
2. 危険源の特定
3. リスクの評価
4. リスク低減策の検討

という手順で実施される. 具体的には, 機械類の使用目的や使用環境を考慮しながら, 危険源を同定し, それらが引き起こすリスクを評価する. その後, 各リスクに対して適切な低減策を検討・実施し, リスクが許容可能な水準に達していることを確認する. RA は, 機械類の設計段階から運用段階まで継続的に実施されるべきであり, 安全性の確保において重要な役割を果たす.

2.2.1 リスクアセスメントシートの概要

また, RA を実施するためのツールとしてリスクアセスメントシート (以下 RA シートとする) がある. RA シートとは, RA を体系的に実施するための支援ツールであり, 設計者や導入者が危険源の特定からリスク評価, 低減策の検討までを一貫して行うことを目的として用いられる. 本研究では, サービスロボットを対象とした RA を実施するために, Excel 形式の RA シートを用いる. RA シートは,

1. 表紙
2. 初期分析・評価シート

3. 方策後再分析シート

4. 基本仕様

以下に各シートを説明する.

2.2.1.1 表紙

表紙では主に、意図した使用、予見できる誤使用、意図した空間/時間制限、リスク見積もりの計算方法を記載する.

対象ロボット名称		実施者		実施日																																																																																	
カフェ配膳ロボットOriHimeD		(立案者、リーダー、チーム参加者、承認者等)		初回 (改訂履歴)																																																																																	
ライフサイクル該当段階	設定(試用)、運搬(通常使用)、保守(トラブル処理を含む)	分析方法(ツール)	種算法(一部加算法を適用)																																																																																		
用途	【設定】 【通常使用】 ①お客さんが注文した飲み物を配膳するために、カフェスタッフは飲み物をロボットの作業トレイ(食せる面)にのせる ②トレイには最大4つの飲み物を置く ③ロボットはタブレットでカフェの環境を確認して、運搬操作をする ④ロボットの動作は前後・回転・音の移動・コマンドによる特定モーションがある ⑤ロボットは飲み物をバックヤードから床へ配膳する ⑥操作者はロボットを通じて床でお客さんと会話する ⑦操作者は必要に応じてロボットにモーション動作をさせる ⑧配膳後バックヤードに戻る ⑨操作者は障害物を回避して、安全に配膳を行う ⑩操作者は体罰を察知しながら時間を計りながら、操作をする ⑪ロボットが障害物を検知したら移動又はモーション動作を停止する ⑫アーム関節部に挟み込みを検知したらモーション動作を停止する ⑬運搬経路を検知したらスタッフ・操作者に知らせる ⑭ロボットは外部から停止するための非常停止ボタンが設置されている ⑮操作者の座席を検知して操作者とスタッフに知らせる ⑯座席のマップを操作画面に表示させる 【保守】 【設定】 【通常使用】 ①スタッフが飲み物を置くときに誤ってこぼしてしまう ②トレイに片寄った位置に飲み物を置くことでバランスを崩す ③床に飲み物が落ちて床に飲み物を置くことで床を汚す ④濡れた手でロボットに触る ⑤濡れた地面を移動する ⑥濡れた床面に飲み物を置くことで、ロボット同士や人間との接触、衝突事故が発生する ⑦道路上に床に飲み物が落ちていたことによりロボットの道路が閉鎖される ⑧お客さんが飲み物を取るときに、こぼしてロボットが濡れる ⑨お客さんが飲み物を取るときに、ロボットが動いてしまう ⑩注文ミスや床番号の間違いによる誤配膳 ⑪運搬経路 ⑫資格のない者がロボットを操作する ⑬長時間操作の疲労による誤操作 ⑭運搬経路による誤作動・故障(音) ⑮ネットワークの脆弱性による遠隔操作の乗っ取り ⑯操作者の操作スキル不足による接触・衝突 ⑰カフェの形状による接触・衝突 ⑱緊急時の操作者の混乱 【保守】 【設定】 ①レストランなどの飲食店内の作業空間の通路や、ホールとキッチン間際の通路のみで使用する。規定のある階段や壁などでは使用しない ②ロボットの使用時間は11:00～19:00(営業時間)(木曜日を除く) ③ロボットは床に貼られた黒線の上を移動する ④距離は利用2時間	リスクの見積/評価基準 リスク見積値: $R = S \times F \times P_s \times A$ <table><thead><tr><th>与えられる頻度又は時間: F</th><th>危険事象の発生確率: P_s</th><th>危害を回避又は制動できる可能性: A</th></tr></thead><tbody><tr><td>連続的/常時</td><td>高い</td><td>4</td></tr><tr><td>頻繁/長時間</td><td>起こり得る</td><td>3</td></tr><tr><td>時々/短時間</td><td>起こり難い</td><td>2</td></tr><tr><td>まれ/稀間的</td><td>低い(まれ)</td><td>1</td></tr></tbody></table> <table><thead><tr><th>危険の大きさ: S</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th></tr></thead><tbody><tr><td>回復に長期治療(1月以上)を要す</td><td>4</td><td>12</td><td>16</td><td>20</td><td>24</td><td>28</td><td>32</td><td>36</td><td>40</td><td>44</td></tr><tr><td>回復に医療措置を要す</td><td>3</td><td>9</td><td>12</td><td>15</td><td>18</td><td>21</td><td>24</td><td>27</td><td>30</td><td>33</td></tr><tr><td>応急手当で回復可能</td><td>2</td><td>6</td><td>8</td><td>10</td><td>12</td><td>14</td><td>16</td><td>18</td><td>20</td><td>22</td></tr><tr><td>対処不要(一時的な痛み等)</td><td>1</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td></tr></tbody></table> <table><thead><tr><th>見積値: R</th><th>評価</th><th>リスク低減の必要性</th></tr></thead><tbody><tr><td>15以上</td><td>リスクは高く、受け入れられない。</td><td>必須、技術的方策が不可欠</td></tr><tr><td>7～14</td><td>リスクの低減が必要。ただし、条件付(他に方策がない、低減が現実的でない)で許容可能。</td><td>必要、技術的方策が困難な場合は警告表示及び管理の方策を講じる * ALARPとして考慮もありえる</td></tr><tr><td>6以下</td><td>リスクは十分に低い。</td><td>不要</td></tr></tbody></table>			与えられる頻度又は時間: F	危険事象の発生確率: P _s	危害を回避又は制動できる可能性: A	連続的/常時	高い	4	頻繁/長時間	起こり得る	3	時々/短時間	起こり難い	2	まれ/稀間的	低い(まれ)	1	危険の大きさ: S	3	4	5	6	7	8	9	10	11	回復に長期治療(1月以上)を要す	4	12	16	20	24	28	32	36	40	44	回復に医療措置を要す	3	9	12	15	18	21	24	27	30	33	応急手当で回復可能	2	6	8	10	12	14	16	18	20	22	対処不要(一時的な痛み等)	1	3	4	5	6	7	8	9	10	11	見積値: R	評価	リスク低減の必要性	15以上	リスクは高く、受け入れられない。	必須、技術的方策が不可欠	7～14	リスクの低減が必要。ただし、条件付(他に方策がない、低減が現実的でない)で許容可能。	必要、技術的方策が困難な場合は警告表示及び管理の方策を講じる * ALARPとして考慮もありえる	6以下	リスクは十分に低い。	不要
与えられる頻度又は時間: F	危険事象の発生確率: P _s	危害を回避又は制動できる可能性: A																																																																																			
連続的/常時	高い	4																																																																																			
頻繁/長時間	起こり得る	3																																																																																			
時々/短時間	起こり難い	2																																																																																			
まれ/稀間的	低い(まれ)	1																																																																																			
危険の大きさ: S	3	4	5	6	7	8	9	10	11																																																																												
回復に長期治療(1月以上)を要す	4	12	16	20	24	28	32	36	40	44																																																																											
回復に医療措置を要す	3	9	12	15	18	21	24	27	30	33																																																																											
応急手当で回復可能	2	6	8	10	12	14	16	18	20	22																																																																											
対処不要(一時的な痛み等)	1	3	4	5	6	7	8	9	10	11																																																																											
見積値: R	評価	リスク低減の必要性																																																																																			
15以上	リスクは高く、受け入れられない。	必須、技術的方策が不可欠																																																																																			
7～14	リスクの低減が必要。ただし、条件付(他に方策がない、低減が現実的でない)で許容可能。	必要、技術的方策が困難な場合は警告表示及び管理の方策を講じる * ALARPとして考慮もありえる																																																																																			
6以下	リスクは十分に低い。	不要																																																																																			

Figure 2.1: cover of RA sheet

2.2.1.2 初期分析・評価シート

初期分析・評価シートでは、危険源の特定とリスク評価を行う。まず、表紙に記載した意図した使用・予見できる誤使用からリスクシナリオを検討し、危険源を特定する。そして、そのリスクが引き起こす可能性のある危害を検討して、表紙の起債に従ってリスクを評価する。その後、各リスクに対してリスクレベルを算出する。その後、リスク項目に対して低減策を検討していく。

2.2. リスクアセスメントの概要

危険源同定						リスク見積						
段階	No.	危険源	危険状態/危険事象	想定危害	対象者	危害の 酷さ S(健康 的な成	危害の発生確率 Ph			リスク 点数 R	備考	
							頻度 F	確率 Ps	回避 A			
配膳・ 移動 (通常 使用)	1	漏電	スタッフが飲み物をロボ ットに置くときに誤って こぼして漏電している状 態で素手で触る	感電死	スタッフ	4	4	1	2	1	16	
	2	移動	操作ミス(押し間違い)に よりロボットが対象者に 衝突する	打撲・転倒	来店者・ スタッフ	2	6	2	3	1	12	高齢者や子供はSを1上げる 疲労時は確率を1上げる 緊急時に操作者が混乱状態の時 は確率を1上げる
	3	熱い配膳物	No.2に加えて配膳物が 奪れて人に掛かる	やけど・不快 感	来店者・ スタッフ	3	6	2	3	1	18	高齢者や子供はSを1上げる

Figure 2.2: analysis of RA sheet

2.2.1.3 方策後再分析シート

方策後再分析シートでは、検討された低減策の効果を再評価する。低減策を実施した後、再度リスクレベルを算出し、その結果が許容可能な水準に達しているか確認する。本研究では、リスクレベルが15以下となるように低減策を検討する。なお、低減策は組み合わせ場合の数値も考慮できる。

初期リスク分析結果			リスク低減					再リスク見積									
段階	No.	危険源	リスク 点数 R	優先 順位	保護方策(メカに よる工学的手段)	方策結果	危害 の 酷さ	危害の発生確率 P _H			リスク 点数 R	保護 方策 組み 合わせ	残留リスク方策(ユーザに依存)			備考(補足説明、参照規格 類、保険等のその他の方 策を記述)	
								頻 度 F	確 率 P _S	回 避 A			警告 ラベ ル	取説書への明記	訓練・管理		保護員他
配膳・ 移動 (通常 使用)	1	漏電	16	1	人が感電しても危 害が小さくなるよう 低電圧で設計	感電しても危害 は低下する	3	4	1	2	1	12	9	ロボットが濡れた 時は絶縁性の 高いゴム手袋を 着用する			
				2	ロボットの電気部 分が濡れないよう にカバーを付ける	漏電しないため 感電の被害が 発生しない	4	3	1	1	1	12					

Figure 2.3: reanalysis of RA sheet

2.2.1.4 基本仕様

2.2.1.5 リスク値の計算

今回使用したRAシートリスク値の計算では積算法(一部加算法)を使用する。この計算方法では、リスク値Rを、危害のひどさSと、危険にさらされる頻度F、発生確率Ps、回避可能性Aの和との積で表す。

$$R = S \times (F + P_s + A)$$

各指標は、RAシートに基づき定性的に評価し、その組み合わせからリスクレベルを算出する。本研究では、リスクレベルが7以上の項目に対して低減策を検討する。

曝される頻度又は時間: F	危険事象の発生確率: P_S	危害を回避又は制限できる可能性: A
連続的/常時 4	高い 4	
頻繁/長時間 3	起こり得る 3	困難 3
時々/短時間 2	起こり難い 2	可能 1
まれ/瞬時的 1	低い(まれ) 1	

危害の酷さ: S	危害の発生確率: $F + P_S + A$									
	3	4	5	6	7	8	9	10	11	
回復に長期治療(1月以上)を要す 4	12	16	20	24	28	32	36	40	44	
回復に医療措置を要す 3	9	12	15	18	21	24	27	30	33	
応急手当てで回復可能 2	6	8	10	12	14	16	18	20	22	
対処不要(一時的な痛み等) 1	3	4	5	6	7	8	9	10	11	

見積値 R	評価	リスク低減の必要性
15以上	リスクは高く、受入れられない。	必須、技術的方策が不可欠
7~14	リスクの低減が必要。ただし、条件付(他に方策がない、低減が現実的でない)で許容可能。	必要、技術的方策が困難な場合は警告表示及び管理の方策を講じる * ALARPとして考慮もありえる
6以下	リスクは十分低い。	不要

Figure 2.4: risk calculation of RA sheet

2.2.2 SafeML(Safe Model Language) とは

SafeML[11] とは、ロボットシステムの安全設計を支援するためのモデリング言語である。SafeML は、SysML を基盤としており、ロボットシステムの安全要件や安全機能を明確に表現できるように拡張されている。SafeML を用いることで、ロボットシステムの設計段階から安全性を考慮したモデルを作成し、安全設計を視覚化する。これにより、ロボットシステムの開発において、安全性の確保が効率的かつ効果的に行えるようになる。具体的には、SafeML は以下の要素を含む。

- Hazard block：危険源を表すブロック
- Harm block：危害を表すブロック
- Harm context block：危険事象や危険状態を表すブロック
- Defence block：リスク低減策を表すブロック
- Defence result block：低減策の効果を表すブロック

各要素の関係を以下に示す。このように、危険源は単体で存在する場合は危害が発生しない。危険源が存在する状況下で危険事象や危険状態が発生することにより、危害をもたらすという因果関係を表現している。

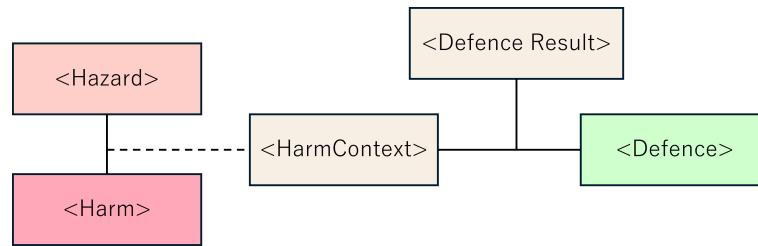


Figure 2.5: SafeML Model

2.3 ロボットシステムの設計工程

本研究では, ロボットシステムを設計する際の参照可能なテンプレートドキュメント作成を目的としている. そのため, 図として設計工程を残すことが出来る SysML を用いた設計工程を参考とする. 以下に SysML の概要と, ロボットシステムの設計工程について説明する.

2.3.1 SysML(Systems Modeling Language) とは

ロボットのシステム設計工程としては, SysML を用いた設計工程がある. SysML[[]] とは, システムエンジニアリングに特化したモデリング言語であり, 複雑なシステムの設計・分析・検証を支援するために開発された. SysML は, UML(Unified Modeling Language) を基盤としており, システムの構造や振る舞いを視覚的に表現できるように拡張されている. SysML を用いることで, システムの要件定義から設計・実装・検証までの各段階で, 効率的かつ効果的にシステム開発を進めることができる. 本研究では以下のダイアグラムを作成する.

- ドメイン構成図
- コンテキスト図
- 要求図：システムに必要な要求を明確化する
- アクティビティ図：システムの動作の流れを明確化する
- ユースケース図：システムが外部に提供する機能を明確化する
- ブロック定義図：システムの構成要素とその関係を明確化する

以下に, 本研究で各ダイアグラムの説明をする.

2.3.1.1 ドメイン構成図

2.3.1.2 コンテキスト図

2.3.1.3 要求図

2.3.1.4 アクティビティ図

2.3.1.5 ユースケース図

2.3.1.6 ブロック定義図

2.4 自動化レベル (Level of Automation)

本研究では, 包括的なユースケースに対して RA を実施していく. その際に, 自動化レベル (以下, LOA とする) を参考にしてロボットを分類してユースケースを検討する. 自動化レベルとは, [] で定義されているロボットを 4 つの項目

- Monitoring : 監視
- Generating : 生成
- Selecting : 選択
- Implementing : 実行

に対して人とコンピュータどちらが担うかで 10 段階に分類した表である. 以下に自動化レベルの表を示す. 本研究では, 遠隔操作ロボットを対象とする. そこで, LOA の表における

Table 2.1: Level of Automation

LEVEL OF AUTOMATION	ROLES			
	MONITORING	GENERATING	SELECTING	IMPLEMENTING
1. Manual Control	Human	Human	Human	Human
2. Action Support	Human/Computer	Human	Human	Human/Computer
3. Batch Processing	Human/Computer	Human	Human	Computer
4. Shared Control	Human/Computer	Human/Computer	Human	Human/Computer
5. Decision Support	Human/Computer	Human/Computer	Human	Computer
6. Blended Decision Making	Human/Computer	Human/Computer	Human/Computer	Computer
7. Rigid System	Human/Computer	Computer	Human	Computer
8. Automated Decision Making	Human/Computer	Human/Computer	Computer	Computer
9. Supervisory Control	Human/Computer	Computer	Computer	Computer
10. Full Automation	Computer	Computer	Computer	Computer

Monitoring と Generating, Implementing の項目に人が関与しているレベルと定義する. すると, レベル 1 からレベル 4 までが該当する. そこで, 本研究では, レベル 1 からレベル 4 までの 4 つの自動化レベルに分類してユースケースを検討する.

第 3 章

RA を組み込んだ設計工程の提案

3.1 はじめに

本章では, 本研究で提案する RA を組み込んだ設計工程と, その適用ユースケースについて説明する.

3.2 従来設計工程の課題

SysML は設計工程の進め方を規定するものではないが, システムエンジニアリングの観点から, 抽象的なシステム要件の定義から詳細な設計までを段階的に進めることが一般的である. 本研究では, 坂本氏らによる SysML の解説書に示されているモデリングの流れを一例として採用し, これを従来設計工程として位置付ける. 設計工程は第 2 章 2.3 節で説明した順番である. 以下に, 順番を示す.

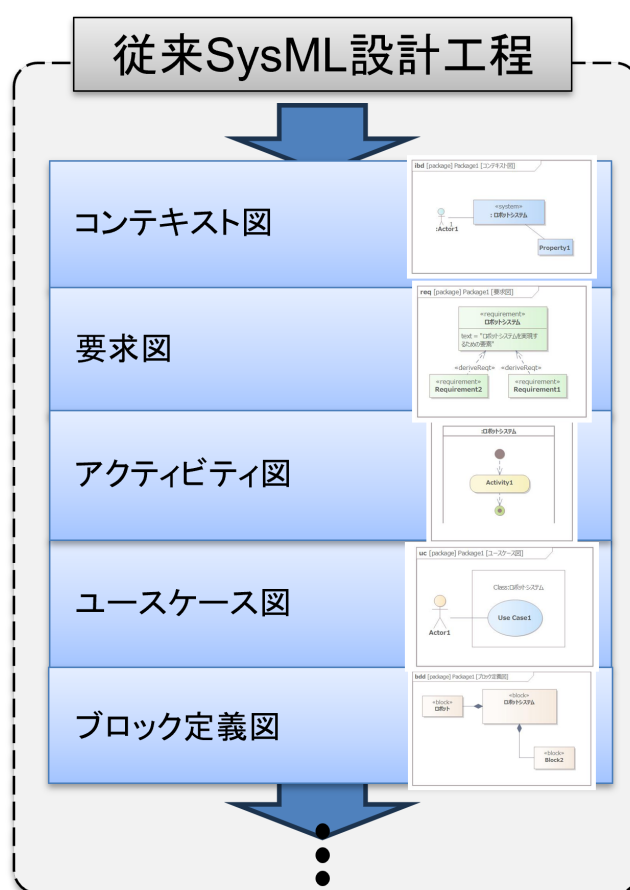


Figure 3.1: sysML

しかし、従来設計工程では、各段階での安全設計に関する指針が明確に示されておらず、設計者の経験や知識に依存する部分が多い。そのため、設計者によっては安全設計が十分に考慮されない場合があり、システムの安全性にばらつきが生じる可能性がある。また、従来設計工程だけでは、安全設計を体系的に進めるための具体的な手法やツールが不足している。これにより、設計者は安全設計を効率的かつ効果的に進めることが難しく、結果としてシステムの安全性が十分に確保されないリスクがある。以上の課題を踏まえ、本研究ではRAを組み込んだ新たな設計工程を提案することで、安全設計を体系的かつ効率的に進めることを目指す。

3.3 新規提案工程の概要

本研究では、RAを組み込んだ設計工程として、SysMLの各図を用いた従来設計工程にRAシートとSafeMLの工程を追加し、安全設計を体系的に進める手法を提案する。以下に提案工程を示す。

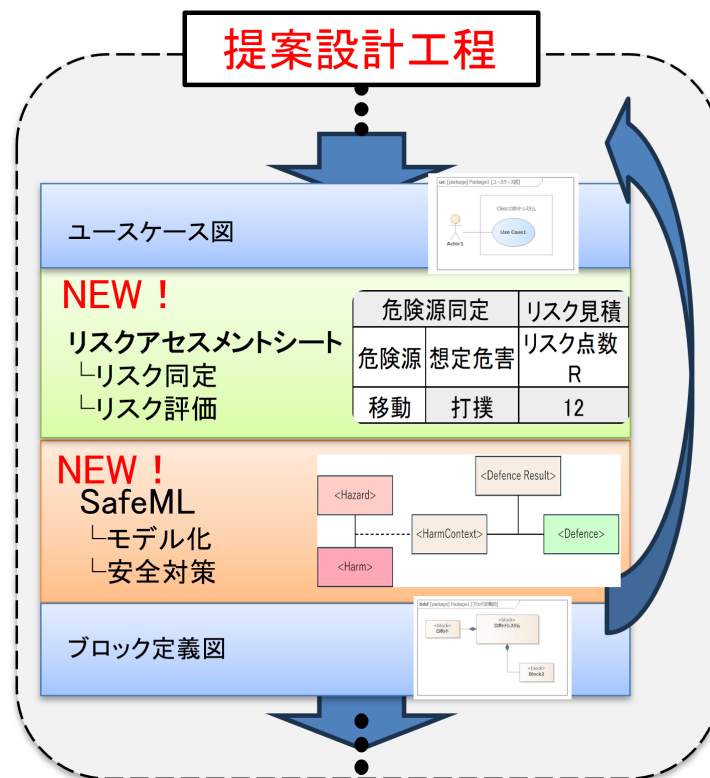


Figure 3.2: 提案設計工程

具体的には, SysML のユースケース図とブロック定義図の間に RA シートによるリスク同定とリスク評価を行う工程, そこで低減策が必要となったリスク項目を SafeML へ図としてモデル化する. そして, 必要となった低減策を SysML の上工程に戻って安全機能を反映する. これにより, システム設計をする中で抽象的なシステム設計から具体的な構成要素を検討する間に規格に沿った安全設計をすることが出来る. つまり, 安全設計の視点からシステムの構造や振る舞いをより明確にし, 安全性の確保を効率的かつ効果的に進めることを目指す.

3.4 各工程の詳細

ここでは, fig で示した提案工程において, 新たに追加した箇所を説明する.

3.4.1 RA シートによるリスク同定・評価

この工程では, 第 2 章 2.1 節で説明した RA シートを用いて, まず, 要求図, アクティビティ図, ユースケース図から意図した使用を検討する. 次に, アクティビティ図を参考にシステム全体の動作からリスクシナリオを抽出していく. さらに, 同定されたリスクにおいて, 2 次被害が発生する可能性がある場合には, そのリスクシナリオも抽出していく. また, リスクの発生原因が複数ある場合は, 原因別にリスクシナリオを記述する. 本研究では, 人に与える物理的なリスクだけではなく, お店に対して信頼性を低下させるようなリスクも対象として同定する. これにより, システムの使用に伴う潜在的なリスクを網羅的に把握することができる. 続いて, RA シート表紙に記載した評価方法で定性的に各リスクのリスク値を算出する. そして, リスク値 7 以上となったリスク項目を SafeML によるモデル化と低減策検討の対象とする.

3.4.2 SafeML によるリスクモデル化

この工程では, 先に述べた RA シートによって対象となったリスク項目を SafeML を用いてモデル化する. 本研究では, SafeML に従って RA シートのリスク項目を表形式からブロックと因果関係を表した線でモデル化する. 具体的には, RA シートの初期段階・評価シートに記載された項目を以下のように,

- 危険源: hazard block
- 危険事象/危険状態: context harm

- 危害：harm block

として表現する。これにより、RA シートの各要素の関係を視覚的に把握できるようになり、また、重複する項目も整理されて、低減策検討が効率化される。低減策を検討した際には、RA シートの方策後再分析シートに低減策を記載して、リスク項目に対して効果があるのか、閾値まで低減できているのかを評価する。さらに、低減策が効果的でない場合には、再度 SafeML モデルを見直し、追加の低減策を検討する。これにより、RA シートによりリスクと低減策を評価し、SafeML によりリスクの因果関係を視覚的に把握することが出来る。その結果、システムの安全性を効率的かつ効果的に確保することを目指す。

3.4.3 安全機能を SysML に反映

この工程では、SafeML で検討した低減策を設計者が必要なものを選び、SysML の上工程に反映する。具体的には、要求図に安全要求として追加し、アクティビティ図でセンサによる回避動作を追加する。操作者を支援するような外部に提供する機能があればユースケース図にも追加する。これにより、RA 規格に沿ってシステム設計をすることが可能となる。また、システムの安全性を設計段階から考慮することができ、結果として効率的にシステム全体の安全性が向上することが出来る。

安全機能を反映した後は、ブロック定義図によりシステムの構成要素を検討する。以降、工程ごとに RA を繰り返すことで、システム全体の安全性を高める。

第 4 章

適用ユースケース

ここでは構築するなにかしらのシステムを説明する.

4.1 対象ユースケースの概要

4.2 自動化レベルの定義

4.3 各LOAのユースケース

第 5 章

提案工程の適用結果

ここでは検証の方法と結果について述べる。ボリュームによって適宜，部や章を分ける。

5.1 ダイアグラム化結果

5.2 同定された危険源・リスク

5.3 設計時の注意点

5.4 考察

第 6 章

納言

6.1 本論文のまとめ

6.2 今後の課題

謝辞

本研究に携わる機会を与えていただき、終始親切なご指導をいただきました名城大学工学部メカトロニクス工学科大原賢一教授に心からの感謝を申し上げます。

参考文献