

信頼性システム



モデリング言語「SafeML」

メタモデル仕様書 Version 2.0



2022 年 6 月

ロボット革命・産業 IoT イニシアティブ協議会

ロボットイノベーション WG

ソフトウェアアーキテクチャ調査検討委員会

発行者 ロボット革命・産業 IoT イニシアティブ協議会

〒105-0011 東京都港区芝公園 3-5-8

機械振興会館 507 号室 日本機械工業連合会内

TEL 03-3434-6571

E-mail office@jmfrri.gr.jp

URL <https://www.jmfrri.gr.jp/>

Copyright © 2022 ロボット革命・産業 IoT イニシアティブ協議会 All Rights Reserved.

本文書は、著作権法および国際条約により保護されています。個人または会社（または会社に準ずるもの）内部での使用を目的として、本文書をダウンロード、印刷、または電子的に閲覧することができます。本資料の内容の全部又は一部については、私的使用又は引用等著作権法上認められた行為として、適宜の方法により出所を明示することにより、引用・転載複製を行うことができます。内容の全部又は一部について、ロボット革命・産業 IoT イニシアティブ協議会に無断で改変を行うことはできません。

ロボット革命・産業 IoT イニシアティブ協議会はいかなる目的においても使用可能性を保証するものではなく、本文書の内容を使用したいいかなる場合においても責任を負いません。本文書の使用者は、本文書に記載された内容の使用に関連して発生したすべての要求、請求、訴訟、損失、損害（人身事故による損害を含む）、費用、経費（弁護士費用を含む）について、ロボット革命・産業 IoT イニシアティブ協議会に何らの損害も与えないことに同意するものとします。

目次

1	はじめに	3
1.1	本仕様書の対象とするユーザ	3
1.2	参考文献	3
1.3	委員名簿	4
2	信頼性システムモデリング言語「SAFEML」サンプルモデル	5
3	SAFEML メタモデル	6
3.1	DEFEND	6
3.2	DETECT	10
3.3	RESPONSIBILITY	11
3.4	REQUIRE	12
3.5	DERIVE	13

1 はじめに

近年のロボット技術の進歩に伴い、ロボットのアプリケーションも幅広くなっている。従来のロボットは工場で柵に囲われた中でのみ作業が行える形での運用が行われてきたが、人協働ロボット、サービスロボットの登場により、ロボットと人との距離が近い中での運用が広く行われるようになってきている。こうした中で、ロボットを適切に運用していく上での安全に対する考え方も拡張していく必要が出てきており、リスクアセスメントを行う際にも多様な条件を検討していく必要が出てきている。従来のリスクアセスメントの方式のように、シート状でリスク要因とその対策を検討整理していく方法は、確実にリスク要因を潰していくことには大きく寄与していくものの、膨大な資料に目を通す必要があり、専門家以外がリスクアセスメントを行っていくにはハードルが高い。今後、多様なユーザがロボットの運用を安全に行っていく中で、リスクアセスメントプロセスの改善やアセスメント結果を把握しやすい形で示すことは重要な課題と言える。

上記の課題に対して、産業技術総合研究所を中心に視覚的に全体像を捉えやすくするモデリング言語の一つとして、SysMLを拡張した「SafeML」の仕様が進められてきていたが、仕様として公開はされていない状況であった。しかし、リスク要因の分析とその対策が視覚的に把握しやすくするという方向性はこれからのサービスロボットなど、幅広いロボットの運用時の安全方策を構築していく上で重要であり、こうした仕様を改善し、オープンにしていくことは、現在サービスロボットの開発・販売をしている企業だけでなく、運用するユーザにとっても大きなメリットがある。

そこで、本仕様は産業技術総合研究所で開発が行われた SafeML 仕様書 1.0 を発展させ、広く利用してもらえるようにすることを目的としたものである。ロボットシステムの安全な運用に向けた方策を練る上で本仕様をご活用いただきたい。

1.1 本仕様書の対象とするユーザ

本仕様書の想定ユーザは、下記のようなユーザの中で、安全設計に関わる者を想定している。

- ロボットハードウェア開発者
- ロボットシステムインテグレータ
- ロボット要素技術開発者・研究者
- ロボット導入者

1.2 参考文献

[SysML] Object Management Group, OMG Systems Modeling Language (OMG SysML), Version 1.6, OMG document number formal/19-11-01, 2019

[Geoffrey] A profile and tool for modelling safety information with design information in SysML:

Geoffrey Biggs, Takeshi Sakamoto, Tetsuo Kotoku: Software & Systems Modeling, ISSN 1619-1366

1.3 委員名簿

(委員長) (学)名城大学
(副委員長) (国研)産業技術総合研究所

(敬称略)
大原 賢一
安藤 慶昭

【委員メンバー】

(株) I H I
I D E C (株)
(学)会津大学
(学)会津大学 復興支援センター
(地独)神奈川県立産業技術総合研究所
川崎重工業(株)
川田テクノロジーズ(株)
国際航業(株)
(国研)産業技術総合研究所
(国研)産業技術総合研究所
セイコーエプソン(株)
セイコーエプソン(株)
(株)セック
(株)セック
T I S (株)
T H K (株)
T H K (株)
(株)東芝
(株)東芝
(株)東芝
(一財)日本品質保証機構
パナソニック(株)
パナソニック(株)
パナソニック(株)
(株)日立製作所
(株)日立製作所
富士ソフト(株)
(株)本田技術研究所
三菱電機(株)
三菱電機(株)
ヤンマーホールディングス(株)
ヤンマーホールディングス(株)
(株)Y O O D S
ロボット革命・産業 IoT イニシアティブ協議会
早稲田大学
【オブザーバ】
(国研)新エネルギー・産業技術総合開発機構

吉光 亮
福井 秀利
成瀬 継太郎
屋代 眞
宮澤 以鋼
蓮沼 仁志
宮森 剛
武田 浩志
花井 亮
中坊 嘉宏
長谷川 浩
林 賢哉
中本 啓之
建部 貴隆
松井 暢之
近藤 裕紀
三好 崇生
貞本 敦史
平山 紀之
山本 大介
駒澤 香介
安藤 健
上松 弘幸
岡本 球夫
中村 亮介
吉内 英也
酒井 貴史
小川 直秀
原口 林太郎
山隅 允裕
杉浦 恒
空閑 融
平泉 一城
北村 篤史
菅 佑樹

赤羽根 亮子

2

信頼性システムモデリング言語 (SafeML：以下 **SafeML**) はシステム設計を行う際に、安全性・信頼性に着目したモデルを記述するためのモデリング言語である。

SafeMLはObject Management Group(OMG：オブジェクト指向技術に関する技術の標準化を行っている国際標準化団体)が標準化を行っているSysML(Systems Modeling Language：システムモデリング言語)をベースとしており、安全性・信頼性に関連する要素をメタモデルレベルで追加定義している。

SafeML を用いて、安全性・信頼性の解析を行った場合の概略サンプルモデルを以下に示す。

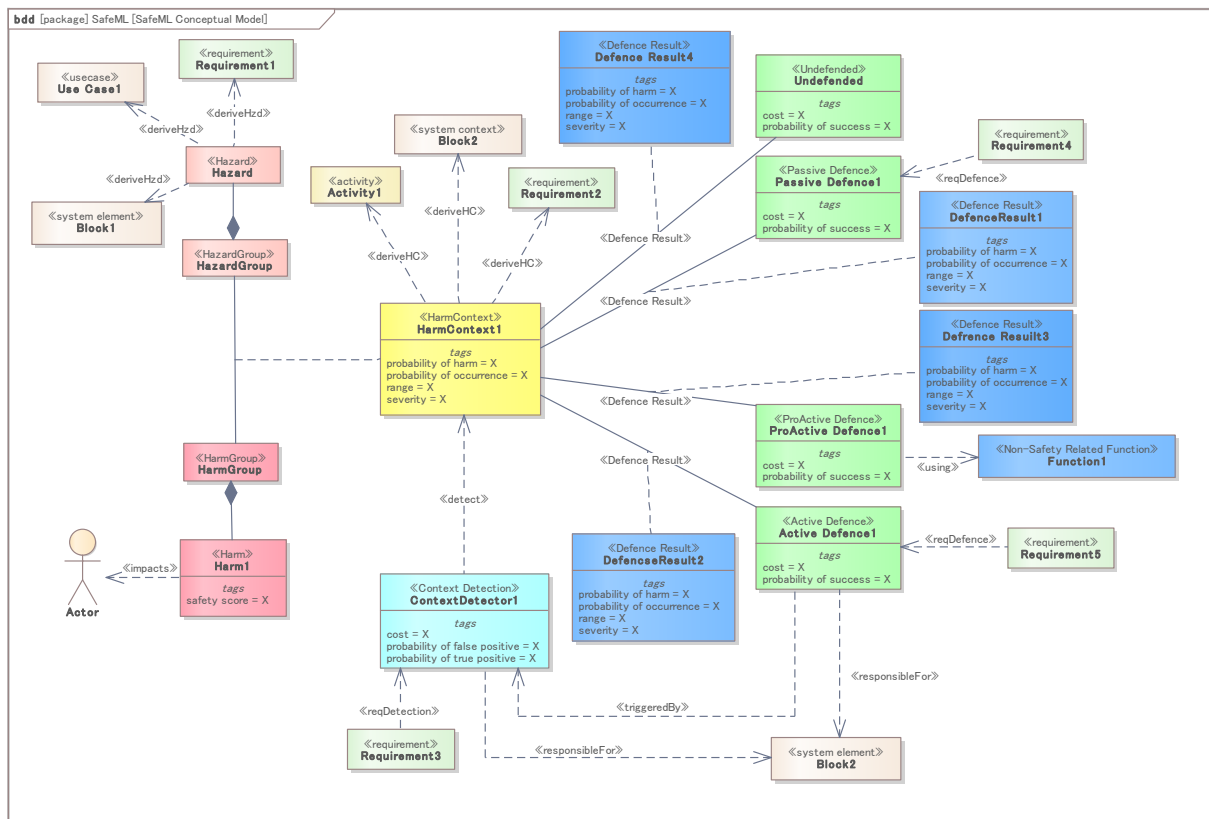


図1 SafeMLを用いた概略モデル

「Hazard」は潜在的に安全性を損なう原因となる要素を表現している。「Harm」とはある場合に実際に危害を加える要素を示している。そして「Hazard」が「Harm」に変化する原因を「HarmContext」として定義している。例えば電気ポットの場合、「Hazard」の例としては、ポットから吹き出す「湯気」が挙げられる。そして「HarmContext」として、「ユーザが体の一部を近づける」が挙げられ、「Harm」として「火傷」となる。危険源である Hazard が存在しても、HarmContext が発生しなければ Harm は発生しない。

なお、ある「HarmContext」が複数の「Hazard」、複数の「Harm」と関係する場合には、「HazardGroup」「HarmGroup」を使用して、関連する要素をまとめて表現する。

次に HarmContext を検出する要素を「ContextDetector」として定義しており、HarmContext と Context Detector の関係を「detect」として定義している。更に HarmContext を発生させないための対策用要素として「Defence」を定義しており、Defence を施した結果、低減された内容を「DefenceResult」として定義している。上述の電気ポットの例では、「ContextDetector」の例としては、湯気の排出口へのユーザの体の接近を検出する「近接センサ」が挙げられる。また「Defence」の例としては、湯気の噴出口付近を覆うカバーなどが挙げられる。

3.1.1. AbstractHazard

Description:	潜在的に存在するユーザや周辺環境に危害を加える原因となる要素を表す抽象クラス		
DerivedFrom:	SysML::Block		
Attributes:	なし		

3.1.2. Hazard

Description:	潜在的に存在するユーザや周辺環境に危害を加える原因となる要素		
DerivedFrom:	SafeML::AbstractHazard		
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.1.3. HazardGroup

Description:	潜在的に危害を加える原因が複数存在する場合、それらをまとめた要素		
DerivedFrom:	SafeML::AbstractHazard		
Attributes:	なし		

3.1.4. AbstractHarm

Description:	ある状態でHazardから発生する実際の被害を表す抽象クラス		
DerivedFrom:	SysML::Block		
Attributes:	なし		

3.1.5. Harm

Description:	ある状態でHazardから発生する実際の被害		
DerivedFrom:	SafeML::AbstractHarm		
Attributes			
Category	String	O	対象要素を整理分類するためのタグ
Safety Score	Real	M	周辺へのダメージを数値化した要素. 算出方法に関しては, 対象システムの用途や設計者の意図に依存する部分が大きいため, 本仕様書では規定していない. 実際にユーザが利用する際に, 別途決定する必要がある.

3.1.6. HazmGroup

Description:	Hazard から発生する実際の被害が複数存在する場合、それらをまとめた要素		
DerivedFrom:	SafeML::AbstractHarm		
Attributes:	なし		

3.1.7. Impacts

Description:	Harmが危害を加える対象を表現する関係		
DerivedFrom:	Dependency		
From:	SafeML::Harm	To:	Actor
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.1.8. HarmContext

Description: 危険源によってユーザや周辺環境がダメージを受ける原因			
DerivedFrom: AssociationClass			
From:	SafeML::Hazard		To: SafeML::Harm
Attributes			
Category	String	O	対象要素を整理分類するためのタグ
Probability of Harm	Integer	M	関連する Hazard および当該 HarmContext が存在した場合に、Harm が発生する確率
Probability of Occurrence	Integer	M	当該 HarmContext が発生する確率
Range	Integer	M	関連した Harm が発生した場合の危害の影響範囲
Severity	Integer	M	関連した Harm が発生した場合の危害の深刻度

3.1.9. Defence

Description: HarmContextの発生を防ぐための防護手段。本クラスは抽象クラスである。			
DerivedFrom: SysML::Block			
Attributes			
Category	String	O	対象要素を整理分類するためのタグ
Probability of Success	Integer	M	防護手段が HarmContext の発生を防ぐ確率
Cost	Integer	O	防護手段を施すために必要となるコスト

3.1.10. Passive Defence

Description: 明示的な起動を必要としない防護手段			
DerivedFrom: SafeML::Defence			
Attributes: なし			

3.1.11. Active Defence

Description: HarmContext の発生を防ぐために、ContextDetector からの情報を用いて、明示的な起動を必要とする防護手段。動作に必要なパラメータは全て設計時に決定され、運用時に調整可能なパラメータは存在しない。			
DerivedFrom: SafeML::Defence			
Attributes: なし			

3.1.12. ProActive Defence

Description: 非安全関連機能 (Non-Safety Related Function) を利用した防護手段、もしくは使用者の防護方策。			
DerivedFrom: SafeML::Defence			
Attributes: なし			

3.1.13. Undefended

Description: 許容できる範囲の HarmContext であるため、防護せずに無視することを示す。			
DerivedFrom: SafeML::Defence			
Attributes: なし			

3.1.14. Non-Safety Related Function

Description: 元々システムが想定しており，備わっておくべき機能(非安全関連機能)			
DerivedFrom: SysML::Block			
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.1.15. Non-Safety Related Detector

Description: システムの機能を実現するために取り付けられた検出手段(センサ). 安全関連機能のための安全センサではなく，元々システムが保持している検出手段.			
DerivedFrom: SafeML::Non-Safety Related Function			
Attributes: なし			

3.1.16. using

Description: ProActiveDefenceが前提としている非関連安全機能 (Non-Safety Related Function) を示す関係.			
DerivedFrom: Dependency			
From:	SafeML::ProActiveDefence	To:	SafeML::Non-Safety Function
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.1.17. triggeredBy

Description: ActiveDefenceが安全機能を実現するために使用している検出機能(ContextDetector)を示す関係.			
DerivedFrom: Dependency			
From:	SafeML::ActiveDefence	To:	SafeML::ContextDetector
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.1.18. Defence Result

Description: 防護手段によって低減された危害の程度			
DerivedFrom: AssociationClass			
From:	SafeML::Defence	To:	SafeML::HarmContext
Attributes			
Category	String	O	対象要素を整理分類するためのタグ
Probability of Harm	Integer	M	Harm が発生した確率. 一般的に, HarmContext に設定された値よりは小さな値となる
Probability of Occurrence	Integer	M	関連する Defence によって低減された HarmContext が発生する確率
Range	Integer	M	関連する Defence によって低減された危害の影響範囲
Severity	Integer	M	関連する Defence によって低減された危害の深刻度

3.2 Detect

HarmContext の検出に関連した部分のメタモデルを以下に示す.

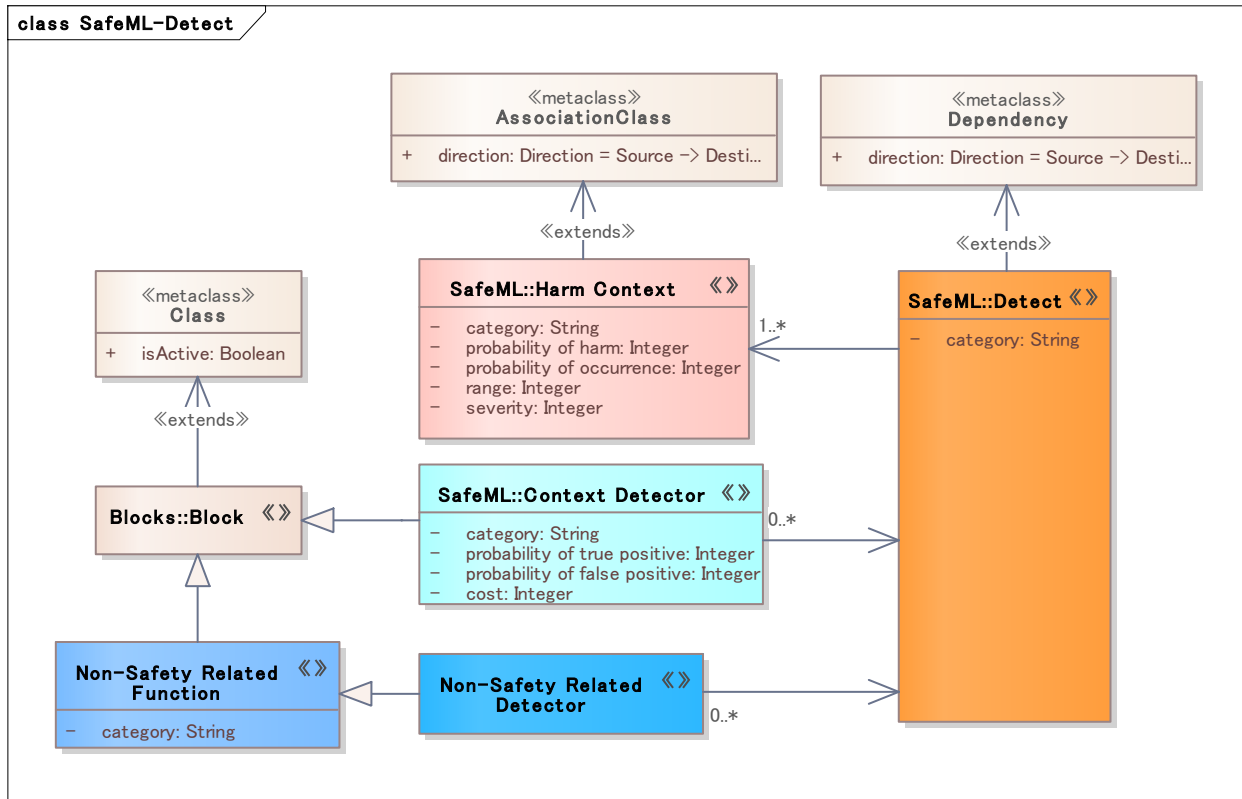


図 3 SafeML メタモデル(Detect)

3.2.1. ContextDetector

Description: HarmContextを検出するための手段			
DerivedFrom: SysML::Block			
Attributes			
Category	String	O	対象要素を整理分類するためのタグ
Probability of true positive	Integer	M	HarmContext が発生した際に、それを正常に検出できる確率
Probability of false positive	Integer	M	HarmContext が発生していないのに、誤検出する確率

3.2.2. Detect

Description: HarmContextを検出手段(ContextDetector)が検出する関係			
DerivedFrom: Dependency			
From:	SafeML::ContextDetector SafeML::Non-Safety Related Detector	To:	SafeML::HarmContext
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.3 Responsibility

SafeML 要素とシステム構成要素の関係に関連した部分のメタモデルを以下に示す。

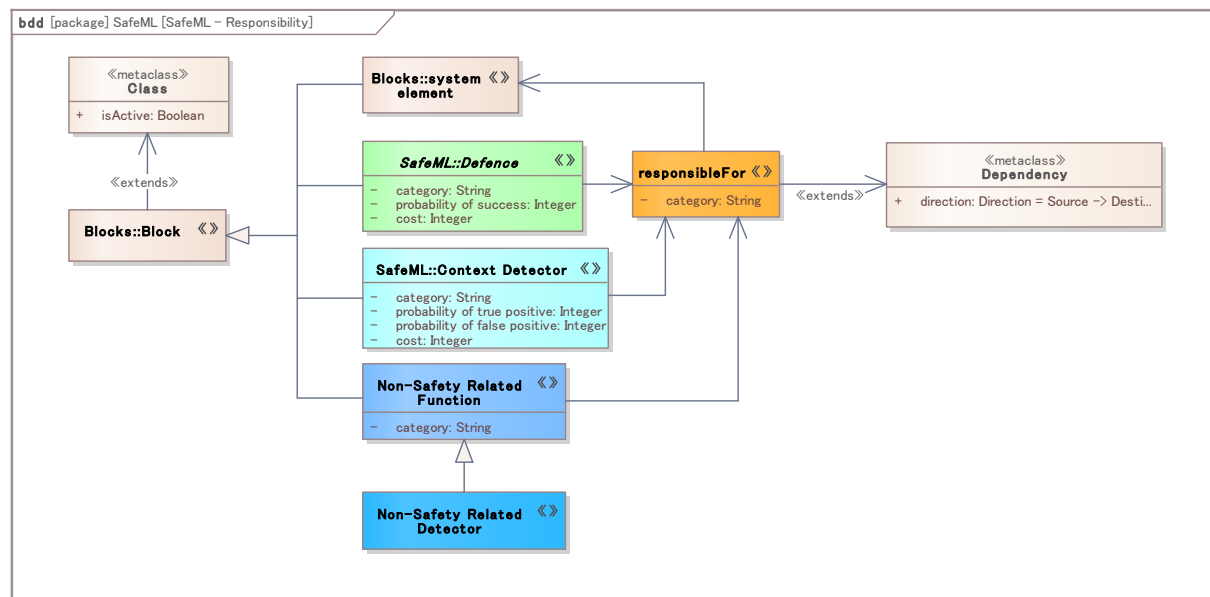


図 4 SafeML メタモデル(Responsibility)

3.3.1. ResponsibleFor

Description: 各種防護手段(Defence), 検出手段(ContextDetector)および非安全機能(Non-Safety Related Function)に対して責任を持っているシステム構成要素を表す関係

DerivedFrom: Dependency

From:	SafeML::Defence SafeML::ContextDetector SafeML::Non-Safety Related Function	To:	SysML::Block(System Element)
--------------	---	------------	------------------------------

Attributes

Category	String	O	対象要素を整理分類するためのタグ
----------	--------	---	------------------

3.4 Require

要求の導出に関連した部分のメタモデルを以下に示す.

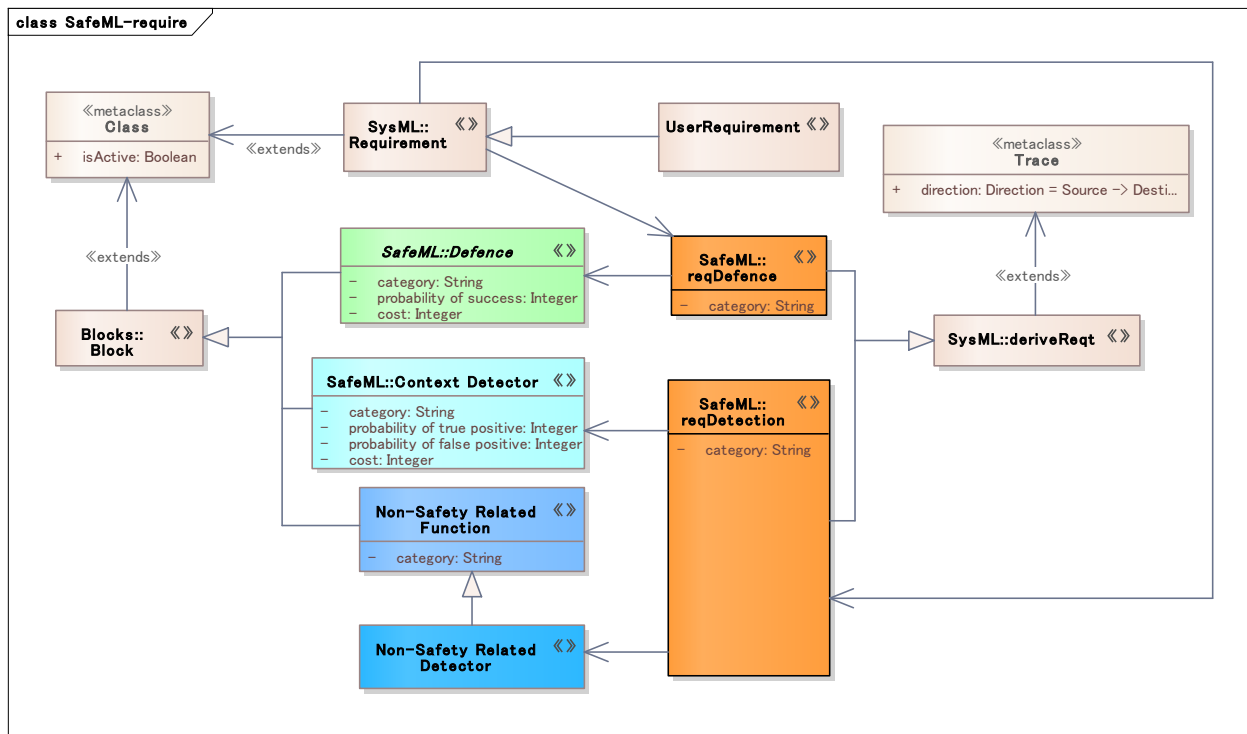


図 4 SafeML メタモデル(Require)

3.4.1. reqDefence

Description: 防護手段(Defence)から導出された要求を示す関係. 各要求がどの防護手段から導出されたのかを示す				
DerivedFrom: SysML::deriveReq				
From:	SysML::Requirement		To:	SafeML::Defence
Attributes				
Category	String	O	対象要素を整理分類するためのタグ	

3.4.2. reqDetection

Description: 検出手段(Context Detector)から導出された要求を示す関係. 各要求がどの検出手段から導出されたのかを示す関係			
DerivedFrom: SysML::deriveReq			
From:	SysML::Requirement SafeML::UserRequirement	To:	SafeML::Context Detector SafeML::Non-Safety Related Detector
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.4.3. UserRequirement

Description: 各種防護手段(Defence)および検出手段(ContextDetector)から導出された要求.
DerivedFrom: SysML::Requirement
Attributes なし

3.5 Derive

要求の導出に関連した部分のメタモデルを以下に示す。

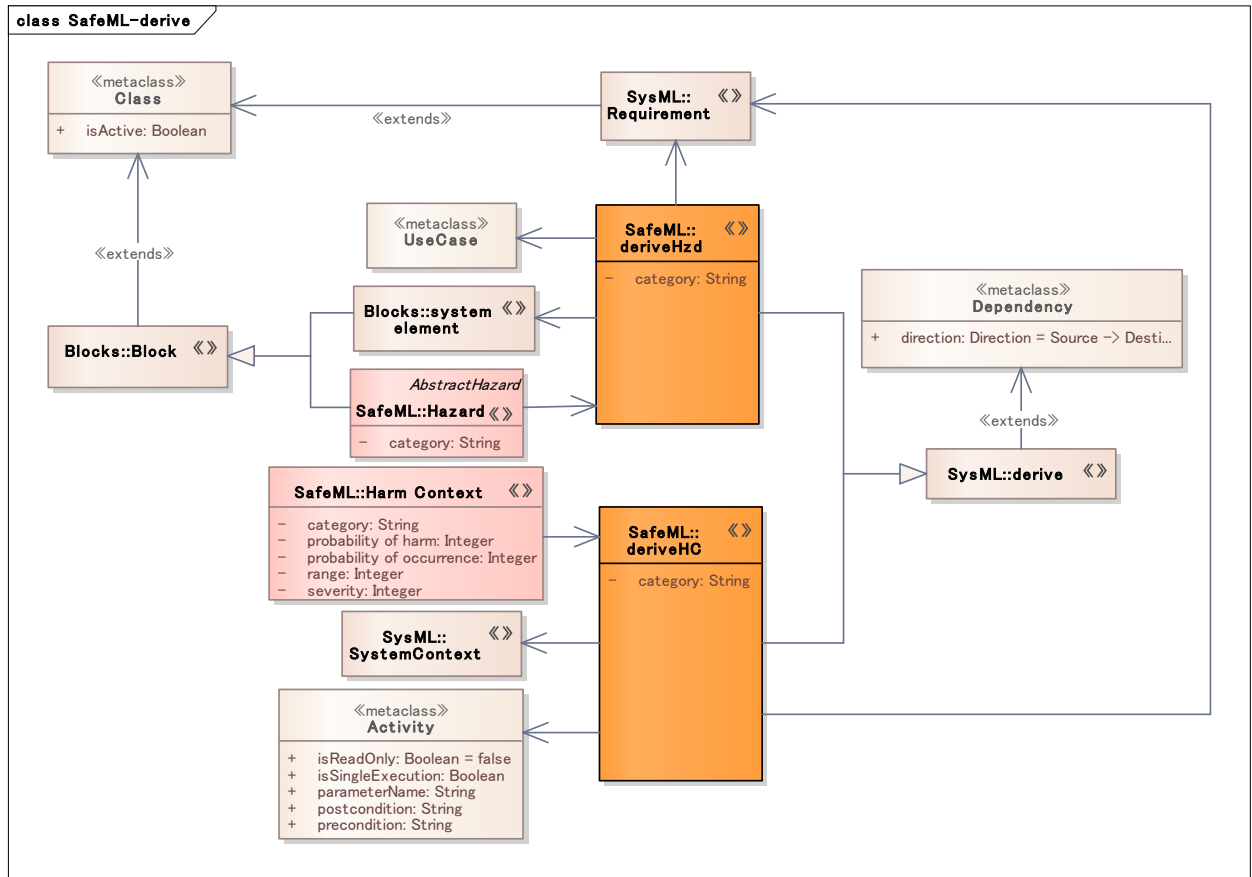


図 5 SafeML メタモデル(Derive)

3.5.1. deriveHzd

Description: Hazardから導出された要素との関係を表現する要素			
DerivedFrom: derive			
From:	SafeML::Hazard	To:	SysML::Requirement, Usecase SysML::Block
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

3.5.2. deriveHC

Description: HarmContextから導出された要素との関係を表現する要素			
DerivedFrom: derive			
From:	SafeML::HarmContext	To:	SysML::Requirement Activity SysML::Block
Attributes			
Category	String	O	対象要素を整理分類するためのタグ

改訂履歴

版番号	公開日	備考
2.0	2022/6/1	第2.0版 (第1.X版については、国立研究開発法人 産業技術総合研究所にて公開された)



ロボット革命・産業IoTイニシアティブ協議会
Robot Revolution & Industrial IoT Initiative