ChangeVision

SCDL仕様書チュートリアル

Safety Concept Notation Open Conference 2016
（SCN-OC 2016）
2016/7/28

SCDL仕様書SWG
株式会社チェンジビジョン 岩永 寿来

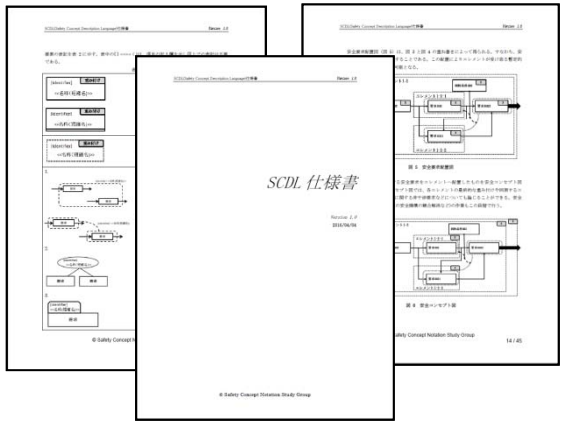
ChangeVision

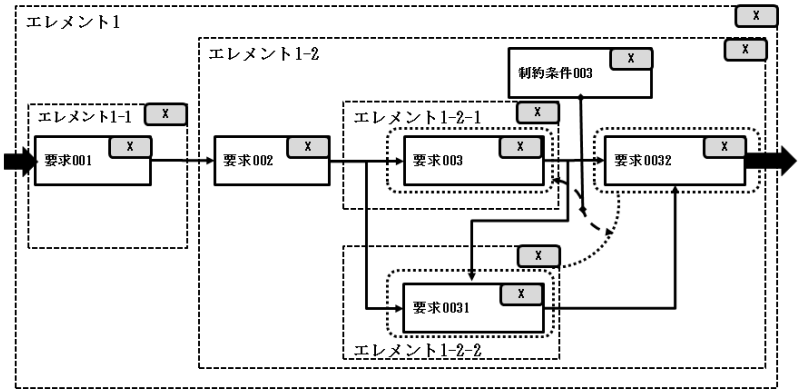
アジェンダ

- SCDLとは
- 他のモデリング言語・手法との関係
- SCDLの記法・文法
- サブワーキング活動内容のご紹介

SCDLとは

- SCDL : Safety Concept Description Language
  - SCDLはシステムの安全設計をアーキテクチャ視点から整理し、論じるための表記法
  - 機能ブロック図、データフロー図ベースの直感的に分かりやすい表記法
  - 表記要素は、数個程度のシンプルな構成
  - 安全アーキテクチャを分かりやすく図解しようとする試みを中心においた、準形式記法





ChangeVision

SCDL仕様書のコンセプト

- SCDL策定のモチベーション
  - システムの安全性をどのようにして設計に織り込んだのか、安全性をどのようにして担保しているのかをシンプルに可視化したい
  - 直感的な要求とエレメントのアロケーション関係や、既存の言語や手法では表現しにくいデコンポジションや非干渉(FFI)をシンプルに表現したい

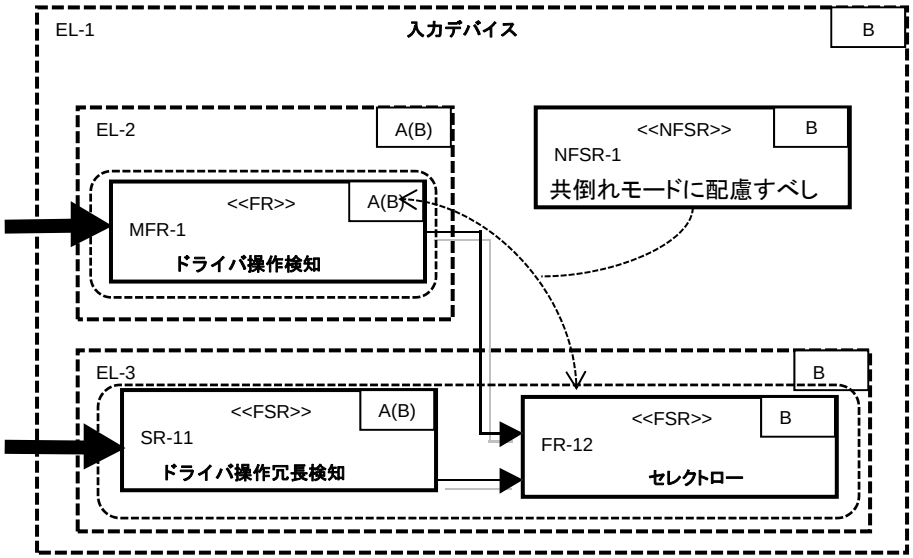
  - 安全設計の検討や論証をアーキテクチャ視点から一貫して連続的にサポートし、理解しやすく安全設計に着目したレビューを支援する言語を策定した

- 対象範囲
  - 61508などに範囲を絞らず、広い分野でのE/Eにおける機能安全についてのアプローチを提供する
    - 現在のメイントピックである26262は、ユースケースで手厚く解説する

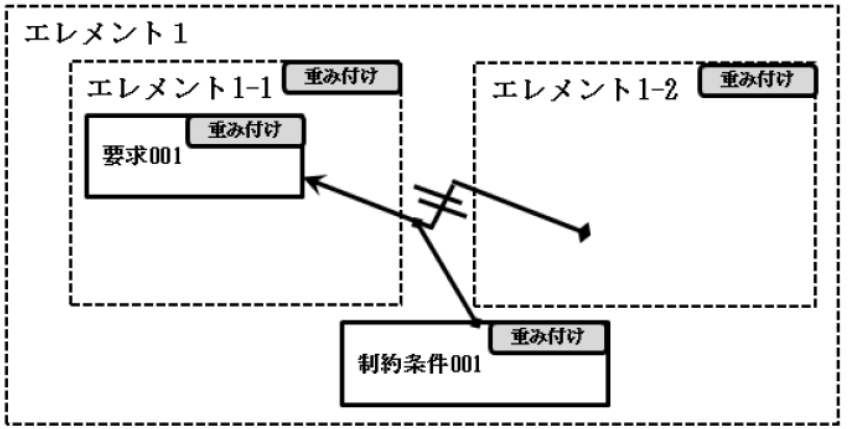
他のモデリング言語・手法との関係(1)

- Q 既存のシステム仕様記述法(SysML, EAST-ADL…)との関係は？
  - 安全アーキテクチャの視点からは、重要ではない文法、表記も多い。よりシンプルに論じられる表記を目指した
  - 他記法では表現しづらい、26262に調度良くあったデコンポジション、非干渉(FFI)をシンプルに表現できる記法が必要と考えた

デコンポジション

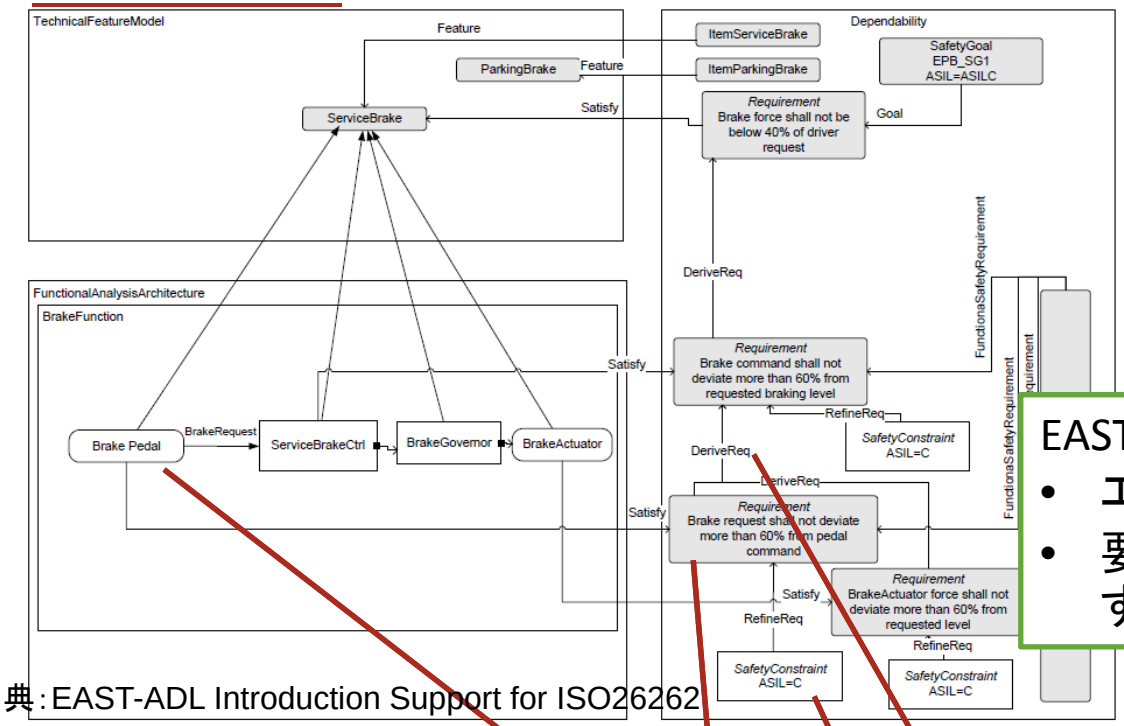


非干渉（FFI）



他のモデリング言語・手法との関係(2)

EAST-ADL

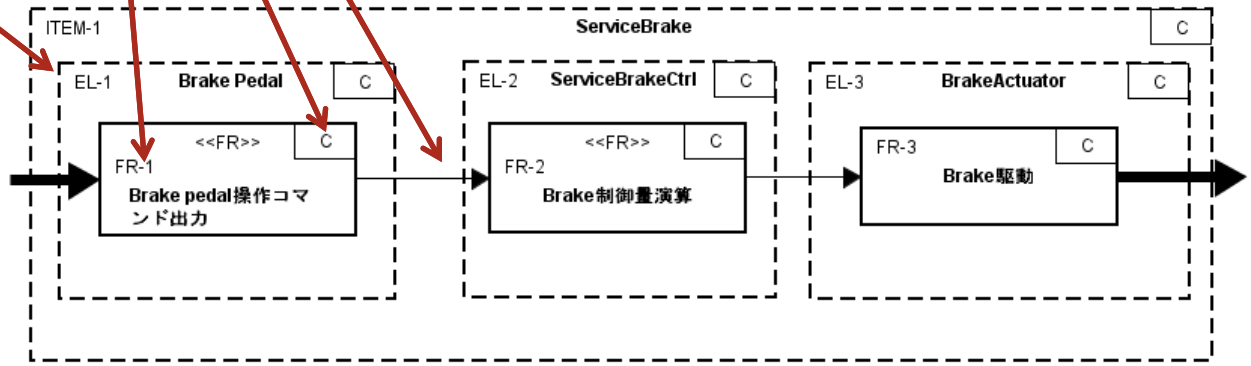


EAST-ADLなどでも十分記述できるが

- エレメントと要求を重ねて表現したい
- 要求間のインタラクションを分かりやすく表現したい

出典：EAST-ADL Introduction Support for ISO26262

SCDL

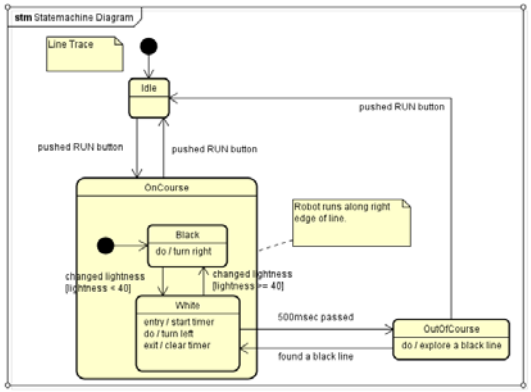


他のモデリング言語・手法との関係(3)

Q SCDLは静的な構造の側面しか扱っていないのでは？

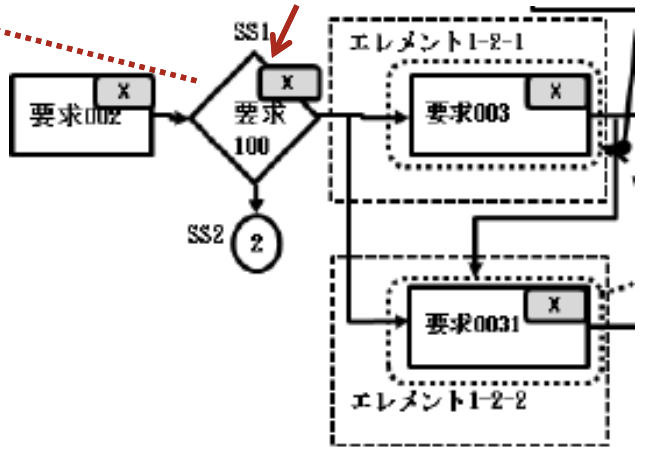
- YES
- あくまでも要求とエレメントの構造しか扱っていない。振る舞いなどの動的な側面は、SysMLなどのしかるべきモデルと紐付けることを想定している
  - すべてSCDLで置き換えられるつもりはなく、補完の関係である

SysML::状態遷移図



SCDL::分岐コネクタ

条件判定や状態遷移により対となる要求構造図をグループ化する際の分岐判定

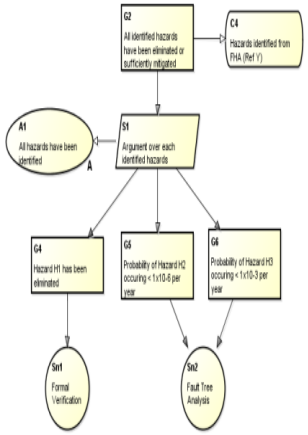


他のモデリング言語・手法との関係(4)

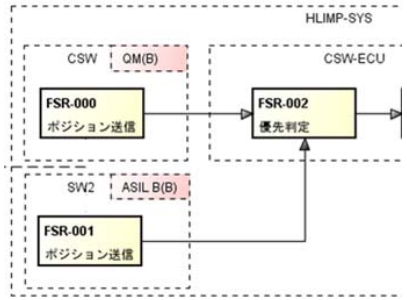
論証
GSN,CAE…

安全性設計
SCDL , SafeML…

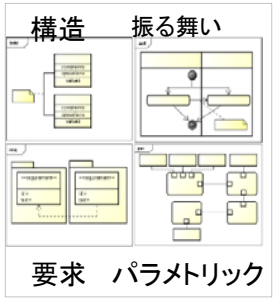
システム設計
SysML, EAST-ADL…



安全設計のアーキテクチャ



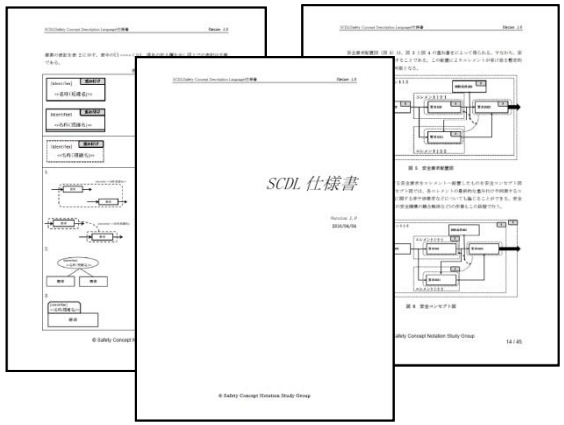
システム設計



H&R,安全性分析
FTA,FMEA,HAZOP,STPA…

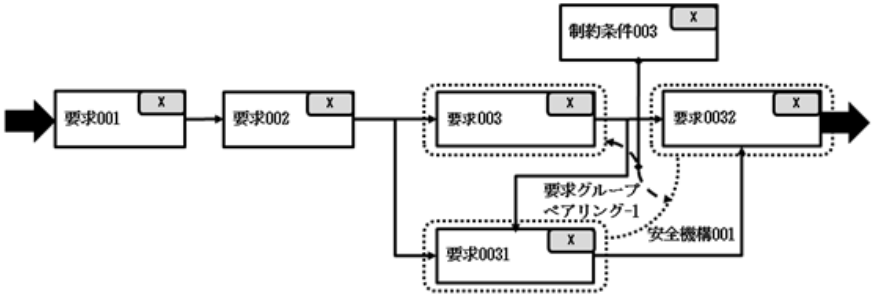
SCDL仕様書目次

- 3章: SCDLとは
  - SCDLと安全設計での役割について概要とコンセプトを示す
- 4章: SCDLの基本定義
  - 最低限必要な要素を定義
- 5章: SCDLの拡張定義
  - 安全アーキテクチャを論ずる主要要素を基本定義、それ以外は拡張
- 6章: SCDLのユースケース
- 付録A: SCDLメタモデル、スキーマー

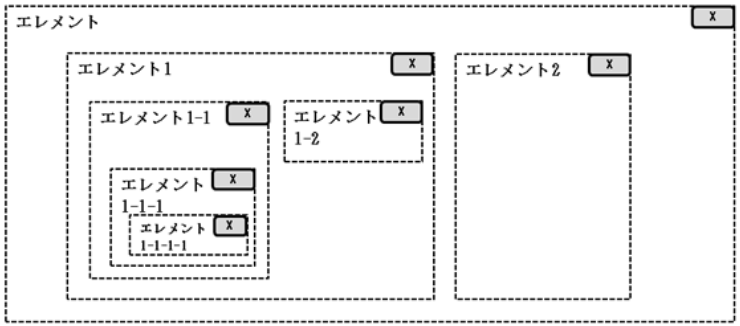


構造図の種類と概要

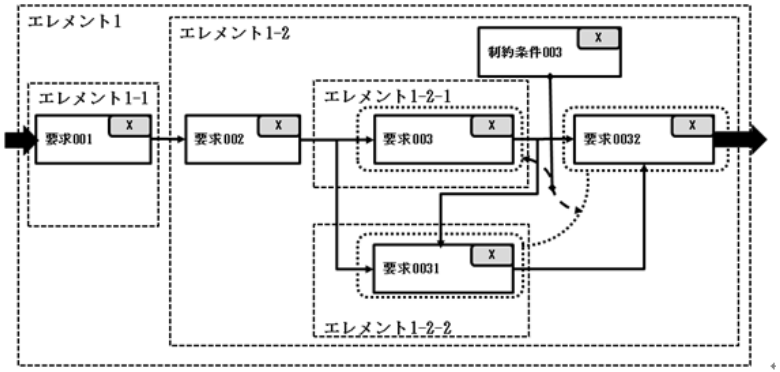
要求構造図
要求の構造を表現



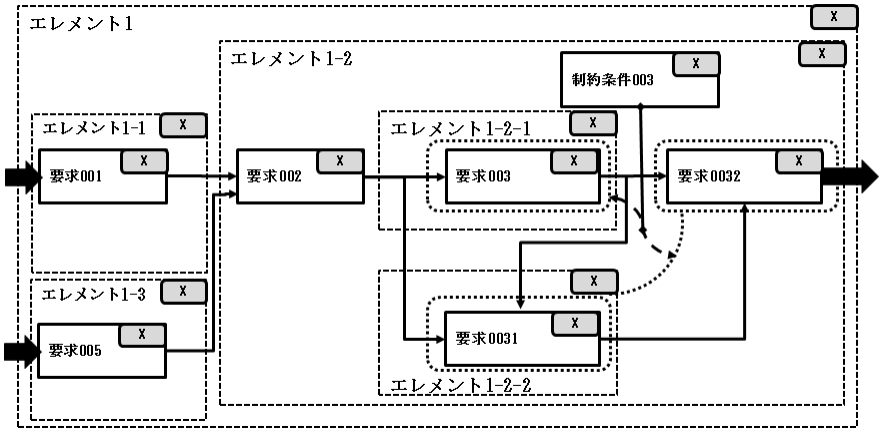
エレメント構造図
要求の受け皿となるエレメント層の構造を表現



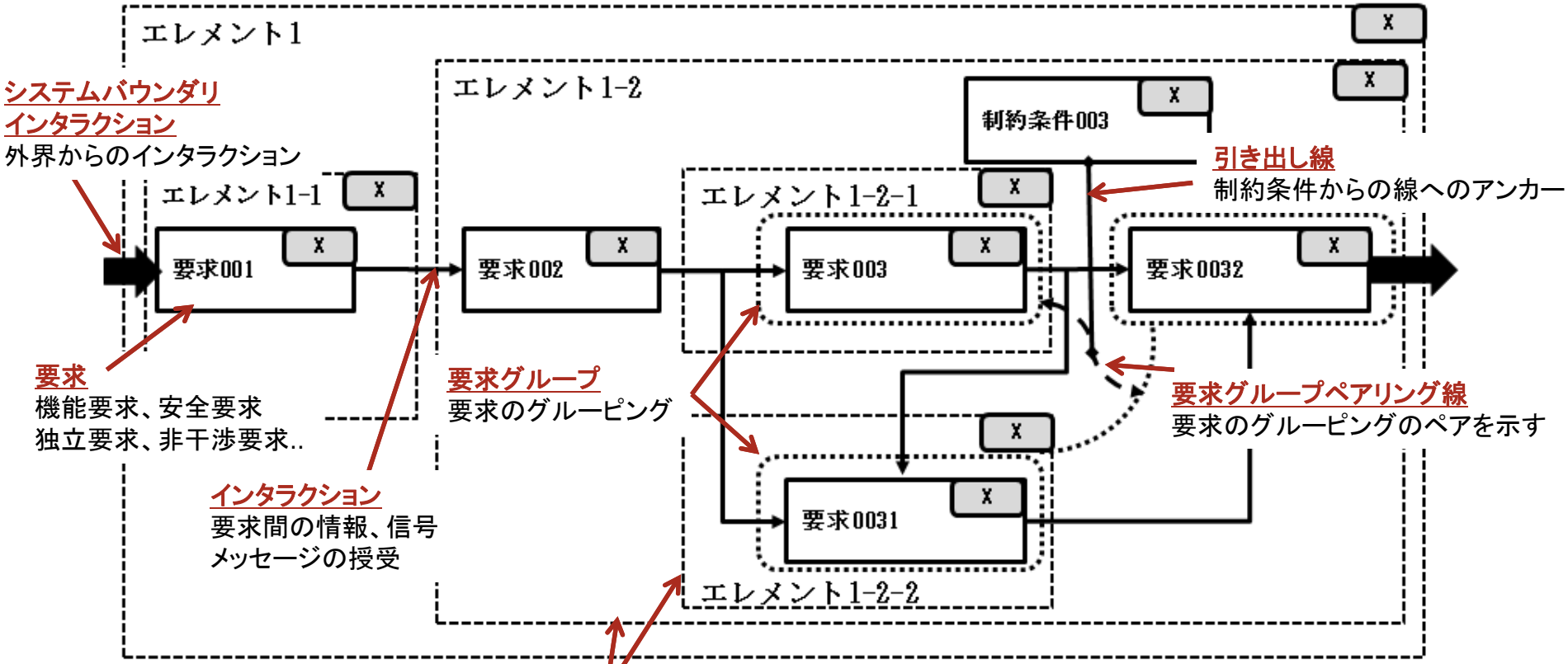
安全要求配置図
要求をエレメントに配置した構造を表現

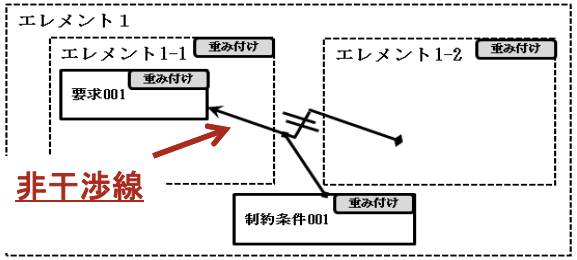


安全コンセプト図
すべての安全機構に関する要求をエレメントへ配置した構造を表現
各エレメントの最終的な重み付けや非干渉要求などを論じ、複数の
安全機構の競合解消など、安全機構の合理化、最適化も行う



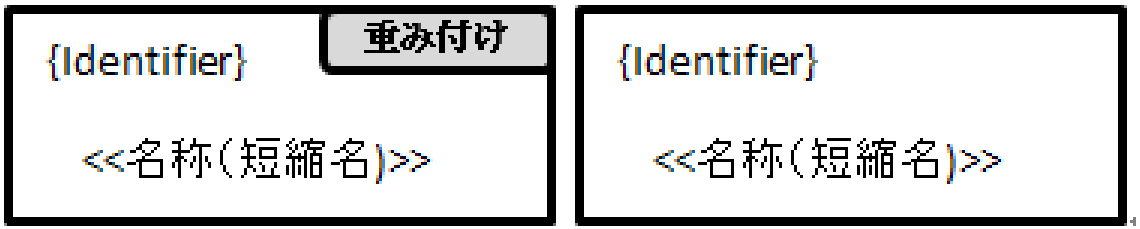
SCDL要素概要


エレメント1
エレメント1-2
制約条件003
エレメント1-1
エレメント1-2-1
要求001
要求002
要求003
要求0032
要求0031
エレメント1-2-2
システムバウンダリ
インタラクション
外界からのインタラクション
引き出し線
制約条件からの線へのアンカー
要求
機能要求、安全要求
独立要求、非干渉要求..
要求グループ
要求のグルーピング
要求グループペアリング線
要求のグルーピングのペアを示す
インタラクション
要求間の情報、信号
メッセージの授受
エレメント
システムの構成要素


エレメント1
エレメント1-1
エレメント1-2
要求001
制約条件001
非干渉線

要求

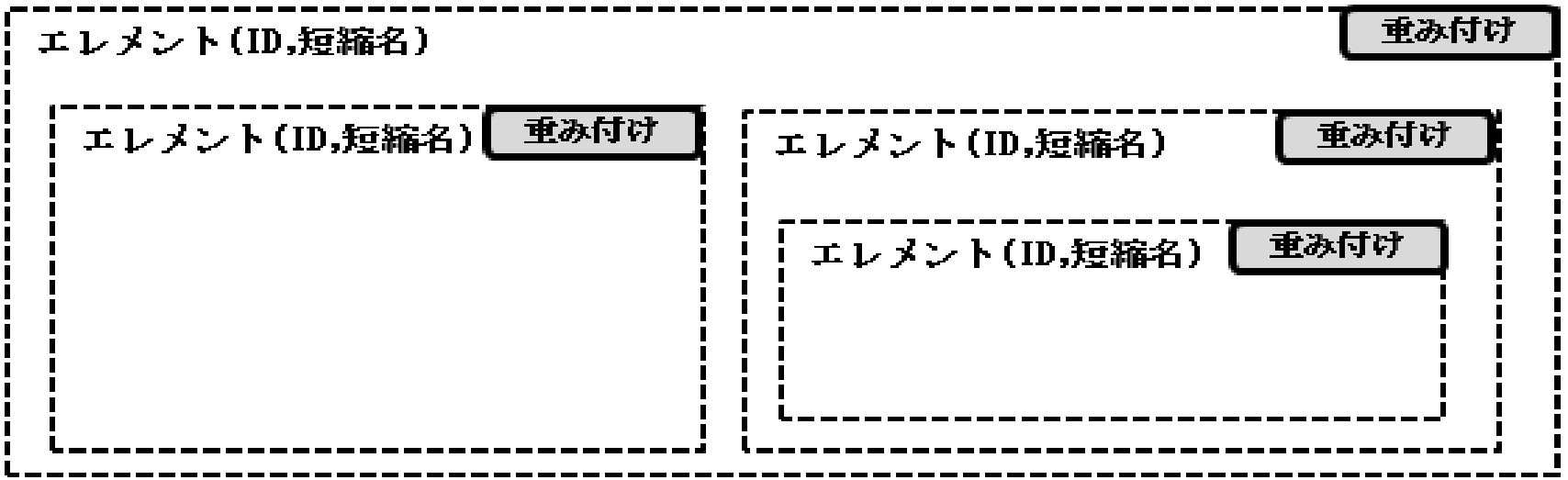
- 要求は長方形で示される
- 一部特定の独立要求、非干渉要求を除き、要求は基本的に機能・役割・振る舞いを扱う
- 要求を示す長方形は、重み付け(ASILなど)を表記する記入欄を右肩に持つ



例

エレメント(1)

- エレメントはシステム、サブシステム、コンポーネント、ユニット、モジュール、パーツ、回路ブロック等および、それらの包括関係を示す
- エレメントを示す長方形は、重み付け(ASILなど)を表記する記入欄を右肩に持つ
- エレメントの線種は任意であるが、要求を示す長方形とは区別できるようにする
  - “すべての記号の線種・太さ・色は任意とするが、それぞれ記号を区別できるように、利用者がルールを規定すること”としている

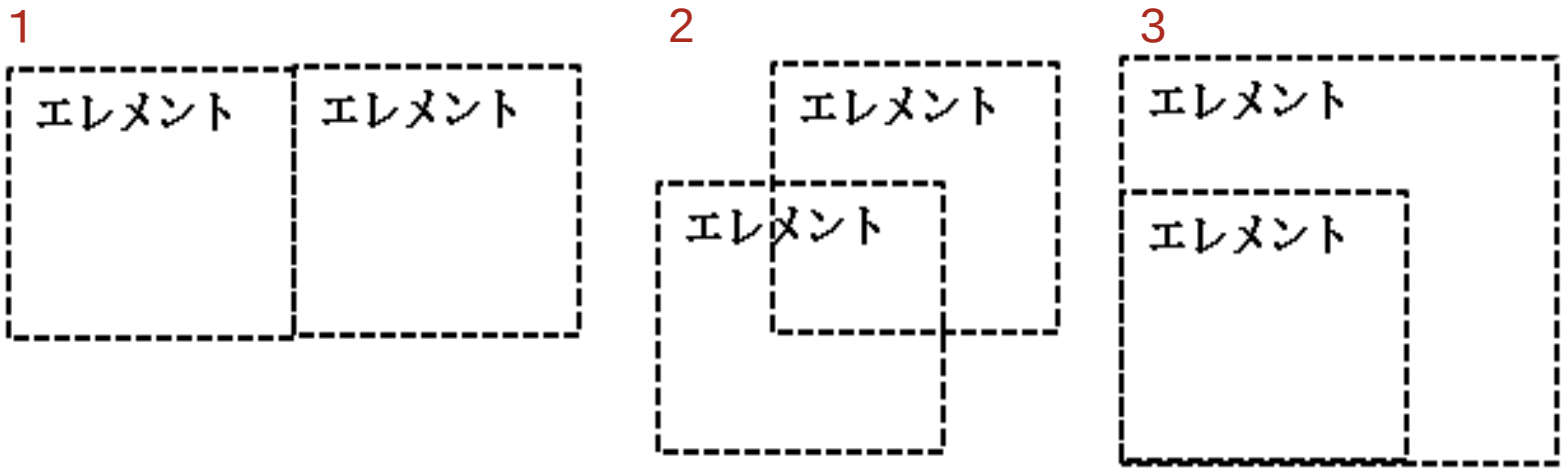


エレメント(2)

エレメント表記の禁止事項

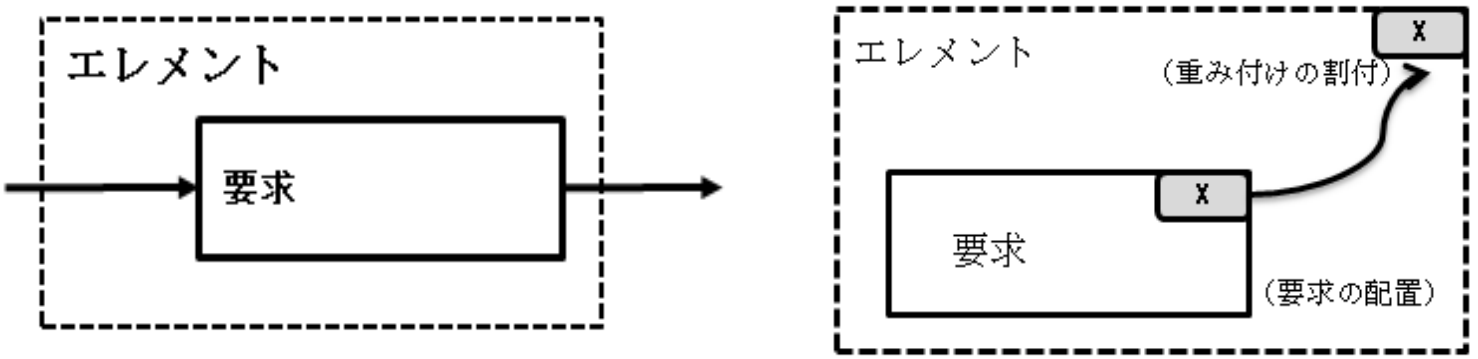
1. エレメント間を線で分割して2つのエレメントとしてはならない
2. エレメントは包括図として表記し、エレメントを部分的に重なる様に表記してはならない
3. 上位エレメントと下位エレメントを内接させてはならない

禁則



要求のエレメントへの配置(1)

- 要求はエレメント内に配置される
- エレメントを示す長方形は、重み付け(ASILなど)を表記する記入欄を右肩に持つ
- エレメントの重み付けは、要求配置の結果として各種安全規格が定める規則に従う。ただし、重み付けの割付が行われるまでは表記されない



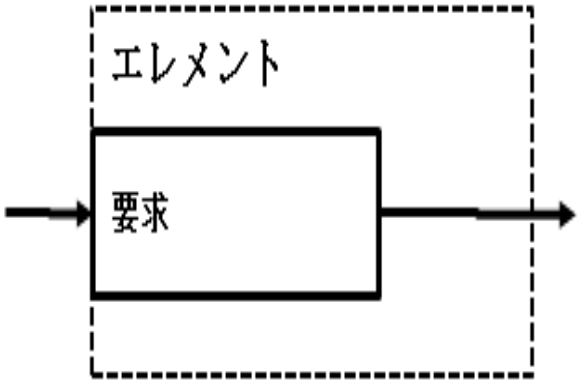
要求のエレメントへの配置(2)

エレメントと要求の配置関係の禁則

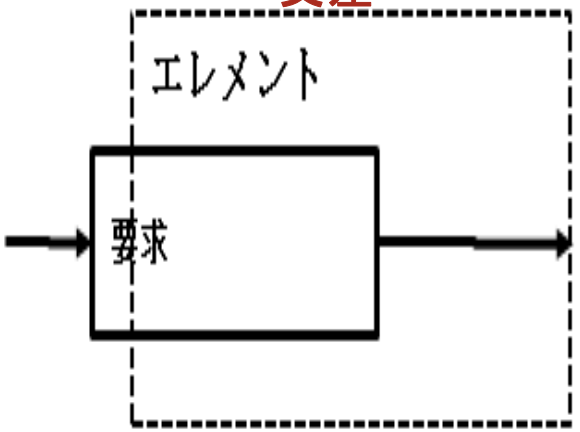
- エレメントの境界線とは内接、交差してはならない

禁則

内接



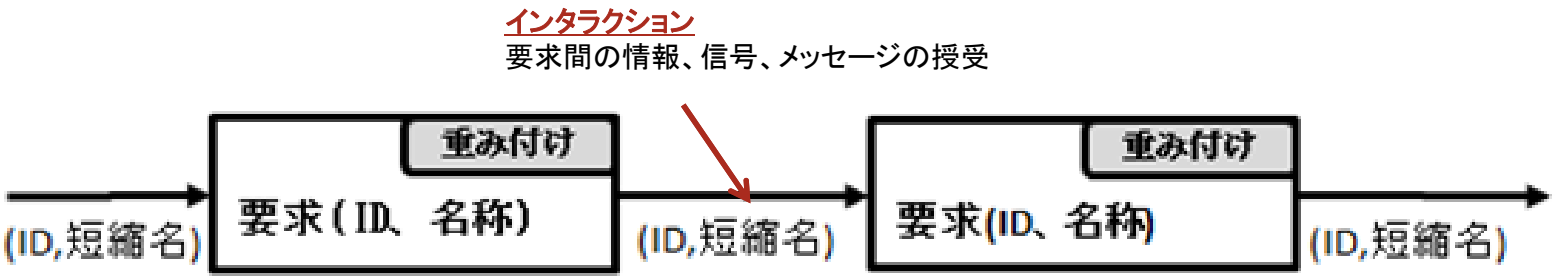
交差



インタラクション(1)

- 要求間の情報・信号・メッセージ等の授受をインタラクションと定義

- 要求を示す長方形は、原則1つ以上の入力と1つの出力で表されるインタラクションを持つ



インタラクション(2)

- 要求は、1つ以上の複数のインタラクション（入力）を持てる

- 同じ情報（インタラクション）を下流の2つ以上の要求で共有する場合は、インタラクションを分岐表記できる

インタラクション(3)

SCDLでは、要求間のインタラクション表記での代表的な禁止事項や例外事項も定義

1. 要求は、要求がアトミックでなくなるため、2つ以上の出力のインタラクションを持ってはならない
2. 入力のインタラクションは、合流のロジック自体を要求化しなくてはならないため、合流表記をしてはならない
3. インタラクションは、アイテム/システム/サブシステムにおいて、一般的に入力部から出力部までつながった経路を持つが、入力のない要求や出力のない要求は例外として存在する（例：初期値設定、乱数発生、リセット等）

禁則

1

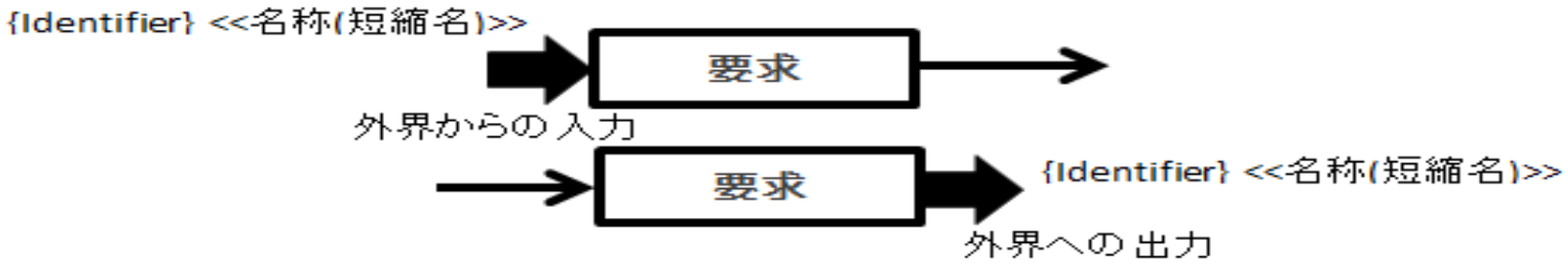
2

例外

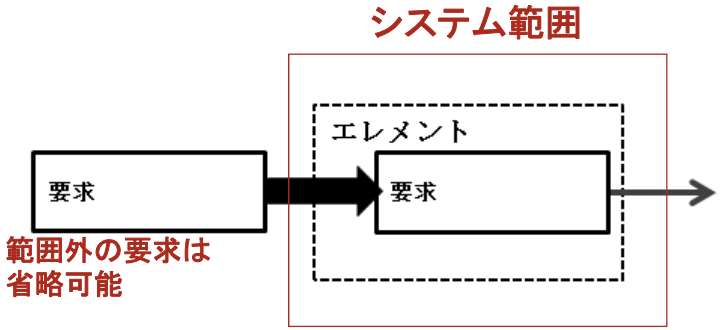
3

システムバウンダリインタラクション

- インタラクションの特殊事例として、システムの外界から、または外界への働きかけを表すインタラクションを、システムバウンダリインタラクションと定義
- システムバウンダリインタラクションは“ブロック矢印“で表現



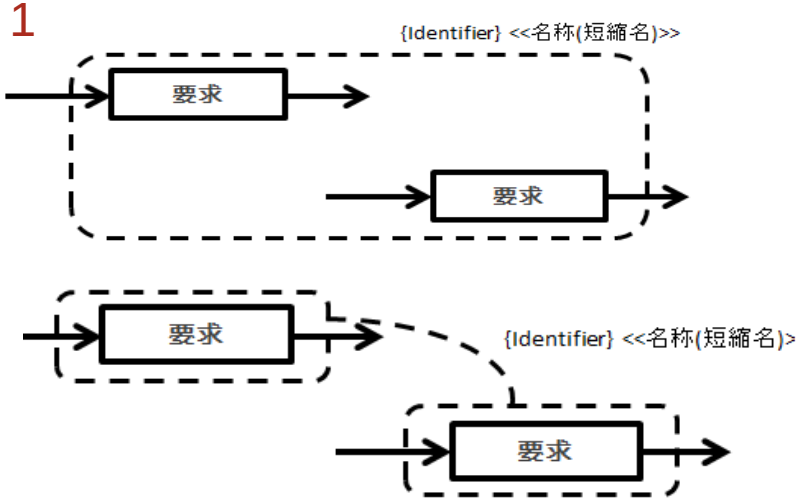
システムバウンダリの範囲外の要求との接続は省略し、どちらかの端点が要求に接続していない表現としてもよい



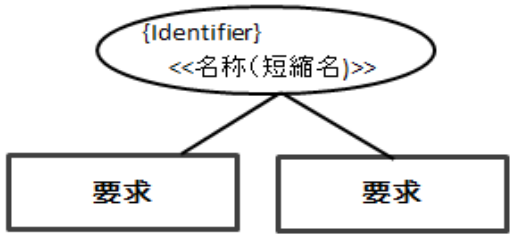
要求グループ

- 要求をグルーピングできる要素を要求グループと定義
- 要求グループは3種類の表記を持つ。どの表記を利用するかは任意とする。
  1. 同じグループに属する要求を枠線で囲む。同じグループであるものを線で紐付けてもよい
  2. 要求グループを楕円で表記し、同グループに属する要求を線で結ぶ
  3. 要求の長方形の上辺にタブを表記し、要求が属する要求グループを表記する

1



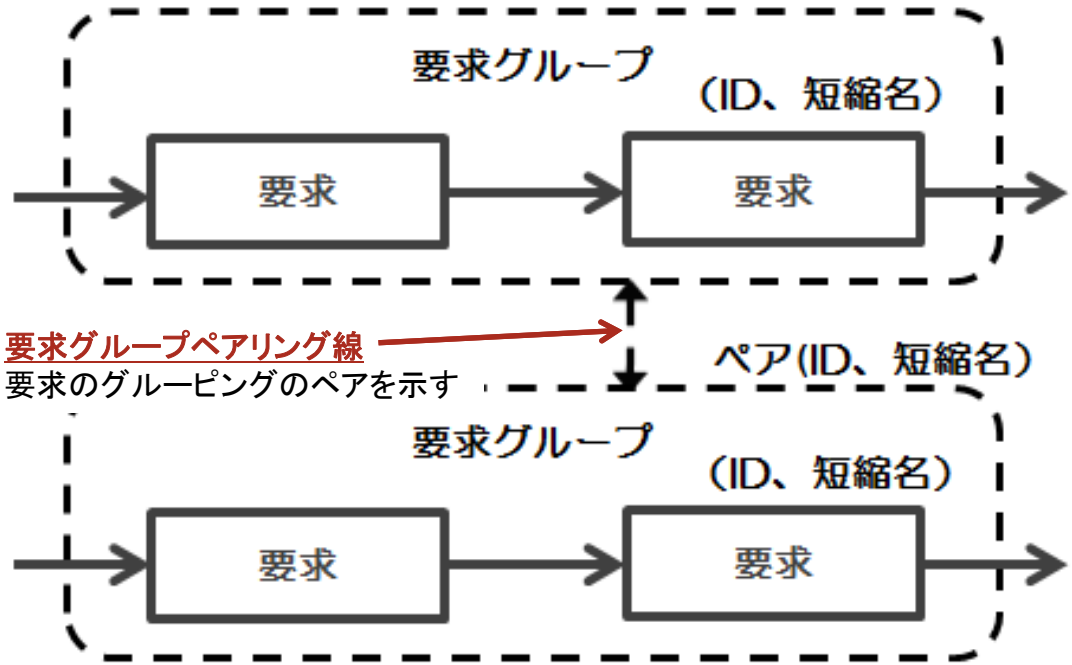
2



3

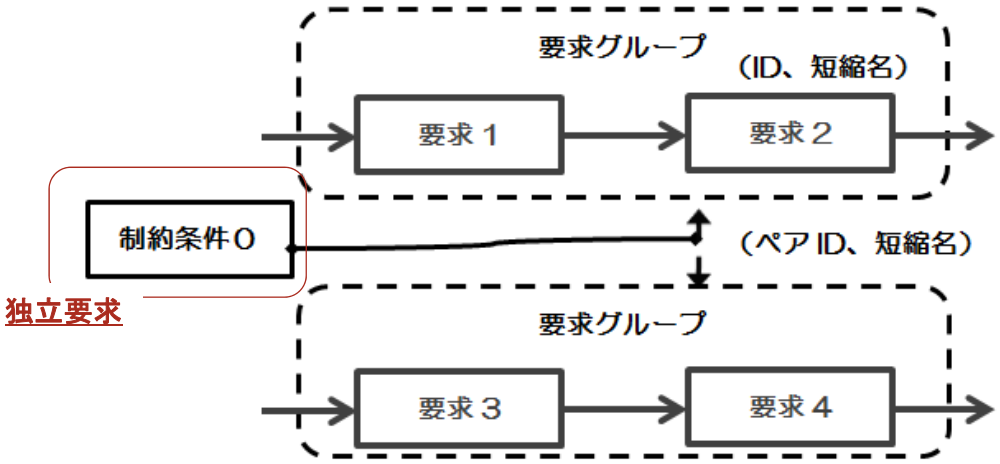
要求グループペアリング(1)

- 冗長な要求グループ間のペアリングは双方向矢印で示す



要求グループペアリング(2)

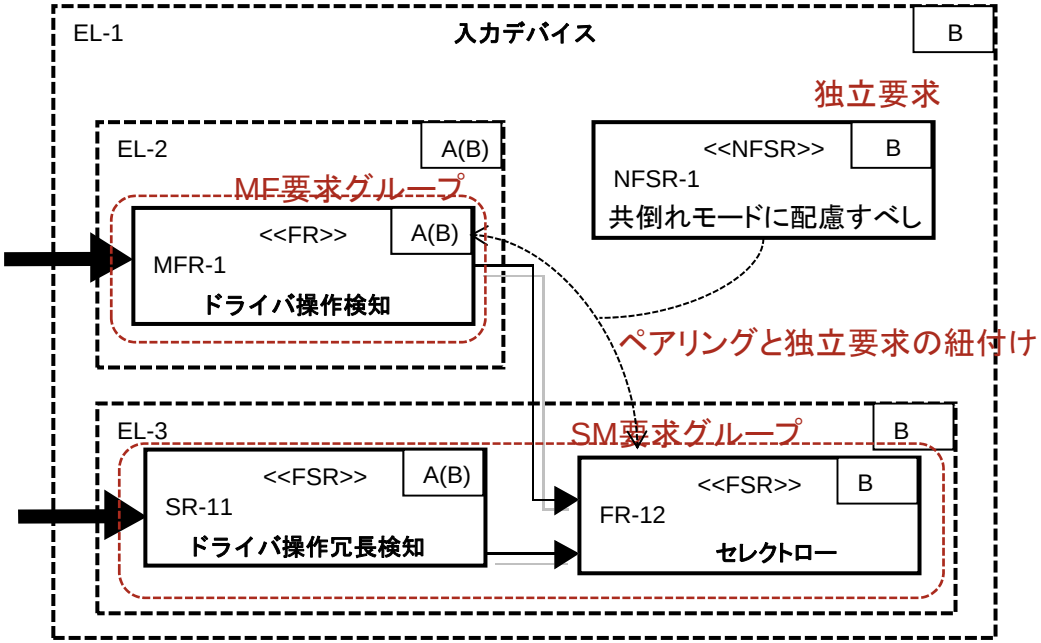
- 独立要求は、制約条件（制約条件は要求を用いる)として、冗長な要求グループ間のペアリングに紐付けて表現する



- エレメントへの配置先が決定されていない、または配置できない場合は、要求の下辺を二重線で表記する

デコンポジションサポート
要求グループと独立要求

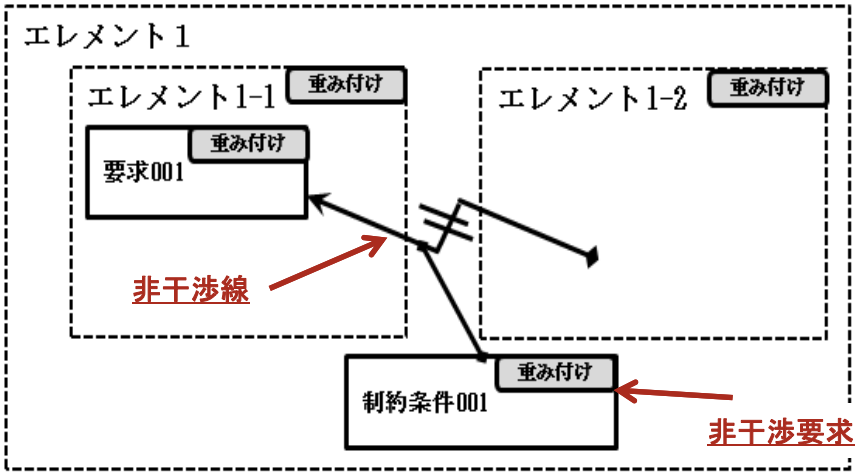
- デコンポジションのサポート
  - 要求のグループ化：デコンポジションにおけるMF/SMグループの指定
  - 冗長な要求(または要求グループ)間のペアリングと独立要求



非干渉線、非干渉要求(1)

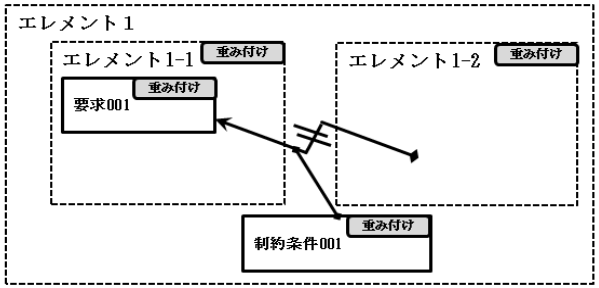
- 稲妻型矢印の非干渉線で、あるエレメントから、他のエレメントに含まれる要求（要求グループ、エレメント）への非干渉を表現できる

- 干渉が存在しないことを非干渉要求として明示し、非干渉線と紐付けて表現できる

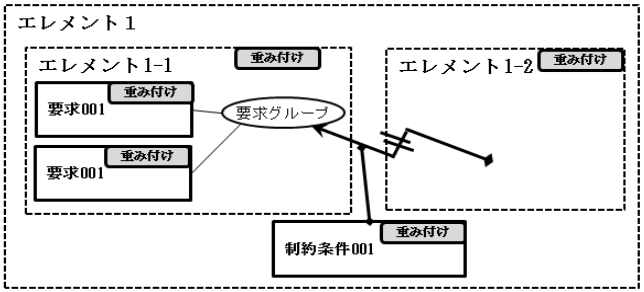


非干渉線、非干渉要求(2)

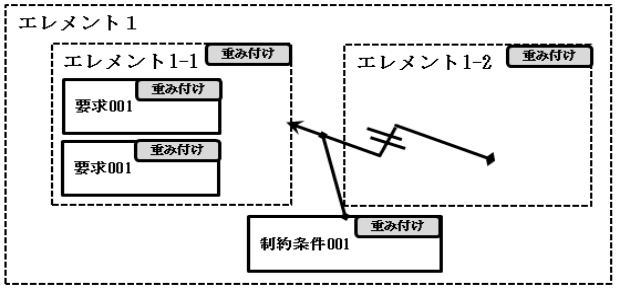
- 稲妻型矢印の非干渉線で、あるエレメントから、他のエレメントに含まれる要求（要求グループ、エレメント）への非干渉を表現できる



エレメント - 要求間の非干渉の表記例



エレメント - 要求グループ間の非干渉の表記例



エレメント - エレメント間の非干渉の表記例

SCDL仕様書サブワーキング 活動内容の紹介

- 今後のロードマップ

2016/4	2017	2018
基本仕様	言語仕様の補強	国際規格提案仕様
V1.0	V2.0	V3.0
SR,ELEMENT,ASILに関する基本表記法を作りこむ	自動車分野のユースケース、メタモデルなど、言語仕様を補強する	国際規格に提案できるレベルに仕上げる

- 東京にて、1,2ヶ月毎に実施
- 次回SWG
  - 第10回 2016/08/10（水） 10:30～14:00 天王州アイル ガイオ・テクノロジー大会議室
  - 第11会2016/09/14（水） 10:30～14:00 天王州アイル ガイオ・テクノロジー大会議室
  - SCDLへの期待や議論など、見学からでもご参加下さい
    - ご興味ある方は、お声掛け下さい

SCDL仕様書ダウンロード

http://www.scn-sg.com/main/