意図記述言語SSQLの狙いと特徴
～安全誘導型設計における意図記述手法～

2017年7月12日
安全性向上委員会　安全仕様化WG
株式会社レンタコーチ
中村　洋

背景

- 安全性向上委員会は2012年度から3年間、意図したものが実現できる要求定義を求めた活動に取組み、2014年度末に成果報告書を公開した。
- 2015年度からは安全仕様化WGに衣替えし、安全が関わる要求を仕様化するプロセスを研究し、それを支援するプロセスモデルと手法を提案する活動を展開している。
- 2016年度には、安全誘導型設計と呼ぶプロセスモデルを重点課題とし、仮想的な電動アシスト自転車開発にその適用を試みた。

目次

要求の仕様化に関する現状と課題

■ 意図が示されない

- 2012年度から3年間、意図したものが実現できる要求定義を求めた活動に取組み、要求の仕様化に関する開発現場における課題をまとめた。
- 顧客との関係では、顧客の意図が示されないこともあるが、それでもソフトウェアは作成できてしまうという課題があった。仕様の間違いに気づきにくいことが問題。

■ 暗黙知は要求として書かれない

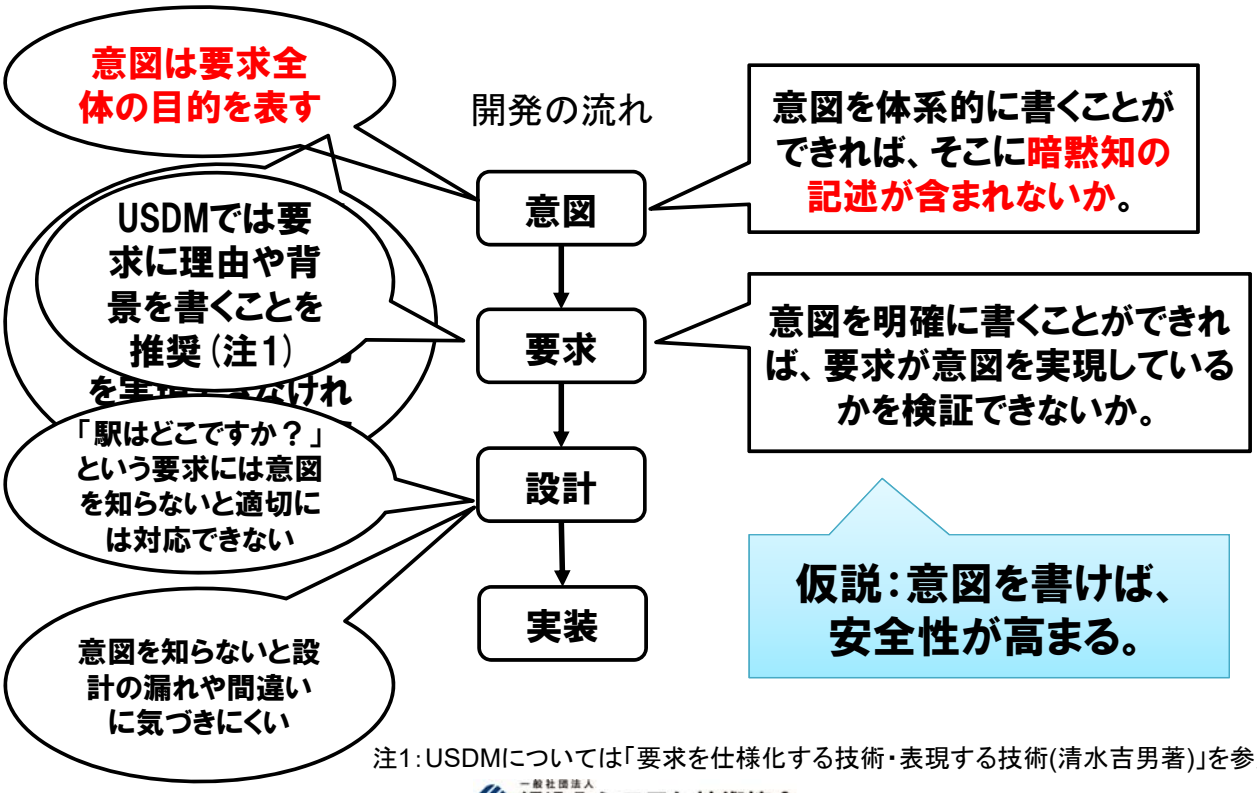
- 顧客側の暗黙の了解、技術的又はビジネス的常識、慣習などが伝わらない現状が、未解決。
- 開発側のオープン化が進むにつれて、意思疎通が一層の課題。

■ 安全実現性の検証が難しい

- 技術と社会の高度化、複雑化が進展。
- 要求段階において意図する安全の実現性を検証したいが、適切な手法が定着していないのが現実。

参照:日経テクノロジーオンライン、「意図を記述すれば、安全性が高まる」

意図の役割



注1：USDMについては「要求を仕様化する技術・表現する技術(清水吉男著)」を参照。

安全誘導型設計の狙い

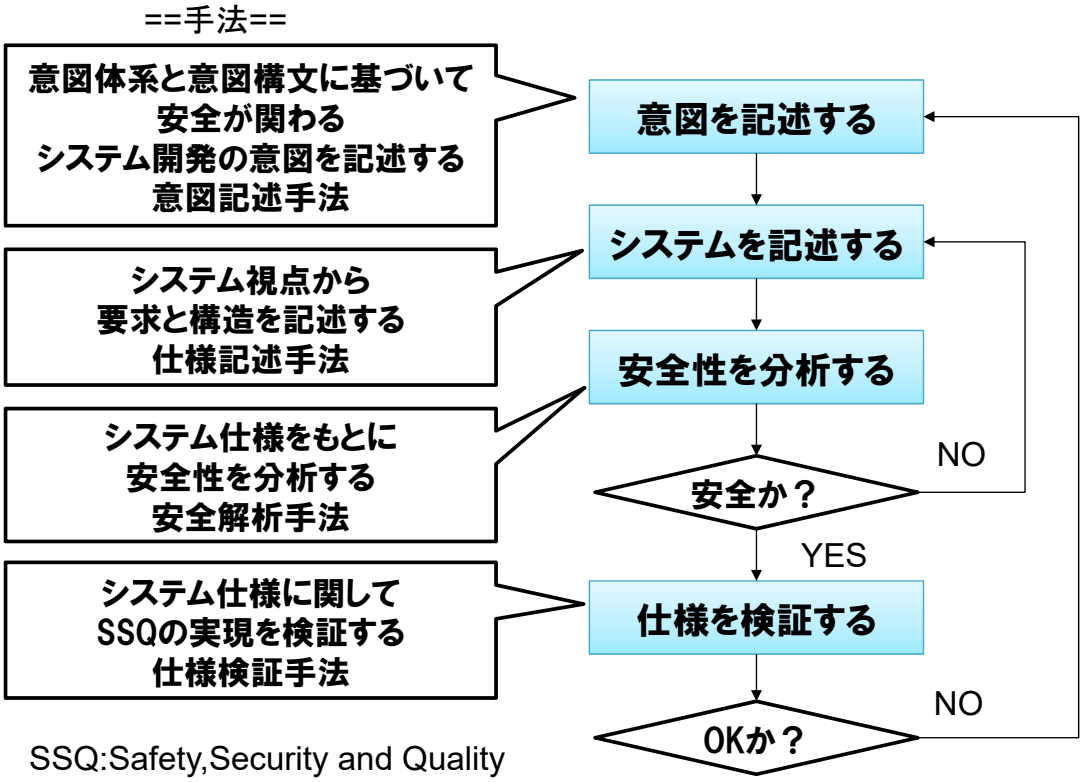
■ 適用分野
- 組込み製品を対象とするシステム開発
- 一般的に、安全が関わるシステム開発

■ 適用プロセス
- システム開発においてコンポーネント設計に先立ち、システム全体の要求を分析し、構造を設計するプロセス

■ 利点
- 要求分析段階において、安全性の検証と安全の作り込みを支援する。
- 要求仕様が意図したことを実現しているかという、意図実現性の検証を支援する。

命名時の思い：
- **意図に照らして、安全か非安全かを判断し、**
- **安全が実現する方向に進めば、要求と構造を適切に設計できる**

安全誘導型設計のプロセスモデル



SSQ:Safety,Security and Quality

試行の概要

- 対象とするシステム開発
  - 仮想的な電動アシスト自転車の開発
- 対象機能
  - バッテリーと自転車本来の機能を除き、電動アシスト機能に限定
- 安全誘導型設計の適用範囲
  - 意図記述
    - 意図体系テンプレートを作成
    - SSQLを用いて意図・要求を記述
  - 安全性分析
    - STAMP/STPA手法を適用
- 参照資料
  - ヤマハ製電動アシスト自転車　PASナチュラL取扱説明書

STAMP:　System-Theoretic Accident Model and Processes
STPA:　System-Theoretic Process Analysis

意図記述言語SSQL：特徴と記述例

意図記述プロセスの概要

■ 狙い
- システム開発の意図に関して、記述すべき視点と事項を体系的に示し、それによって記述漏れの防止を図る。
- 曖昧さを排除して記述の正確性を高め、あわせて、整合性などの検証を可能とする。
- 意図と要求の追跡性を可能とする。

■ 意図体系
- 標準的な意図体系フレームワーク
- 適用分野固有な意図体系テンプレート

■ 意図構文
- 意図記述言語SSQL
- 要求記述ツールSLP
- EARSパターン、テンプレート

■ 意図と要求の追跡性
- ゴール構造表記法GSN
- SysML要求図

SSQL ： SSQ’ s intention describing Language
SLP: Spec Logical Perfect
EARS:Easy Approach to Requirements Syntax
GSN: Goal Structuring Notation

SSQLの概要

- 目的
  - システム開発に関する意図を記述するための構文を提供する。
  - 意図体系テンプレートの記述を可能にする。
  - 既存の処理系の活用を可能にする。
- 特徴
  - テンプレートに沿って意図とそれに関連する要求を記述できる。
  - EARSパターン相当の要求記述構文が使用できる。
  - SLPテキストへの変換によってSLP処理系が活用できる。
- 意図・要求構文
  - 一般型2種：意図と要求の記述構文
  - EARS型4種：EARSパターン準拠の要求記述構文
- コメント構文
  - SSQLコメント：意図体系テンプレートを記述するため
  - SLPコメント：SLP言語に同じ

SLP処理系は、JFP社が販売しており、構文化された要求を処理できる

意図をSSQL構文で記述できるか？

要求する、規定する、又は選択する意図	if(主語、述語) 目的語、述語
新年度セールスの目玉として販売する。	新年度セールスの目玉/本製品にする
主婦が自分の判断で購入できる。	購入可否/主婦が一人で判断できる
トップブランドの地位を維持する。	ブランド地位/トップ状態に維持する
自然で滑らかな乗り心地を実現する。	
坂道でもパワフルで滑らかな乗り心地を実現する。	
目的外使用に関わる安全にコストをかけない。	if(使用目的/規定範囲以外である)　安全コスト/配慮しない
利用拡大のために法的制約を避ける。	
発生件数が多い事故を避ける。	多発する事故/避ける
アシスト力が急に大きくなることに慣れない。	if(アシスト力/急に大きくなる)　アシスト機能/利用者が慣れないと感じる
高速度での衝突による衝撃を回避する。	if(走行速度/高速である)　衝突による衝撃/回避する

目的語は何か？

条件はあるか？

表現は自由だが、曖昧さが残る

構文化され、不自由だが曖昧さはない

文

	構文規則	SLP変換
記述文	(空白) 意図・要求構文	対応するSLP表現
SSQLコメント文	文字列	(:文字列
SLPコメント文	(:コメント	同左

先頭文字で文を区別する:
空白 -> 記述文
(-> SLPコメント文
それ以外 -> SSQLコメント文

SLPインポートツール:
SSQLテキストを読み込み、
SLP変換を施し、その結果を
SLP処理系に渡す

文の区切りは改行

意図・要求記述構文

		構文規則	SLP表現
一般型		x/P	Do <x>を{P}とせよ
		if(y/Q) x/P	if <y>が{Q}ならば then Do <x>を{P}とせよ else Do nothing endif
EARS型	事象型	when(y/Q) 一般型	if <y>が{Q}という事象が発生したならば then 一般型表現 else Do nothing endif
	状態型	while(y/Q) 一般型	if <y>が{Q}という状態にあるならば then 一般型表現 else Do nothing endif
	環境型	where(y/Q) 一般型	if <y>が{Q}という環境にあるならば then 一般型表現 else Do nothing endif
	問題型	case(y/Q) 一般型	if <y>が{Q}という問題があるならば then 一般型表現 else Do nothing endif

備考:xとyは名詞。Pはxを目的語とする述語部、Qはyを主語とする述語部。
ここで、述語部とは、一つの文の中で主語又は1つの目的語を除く残りの部分とする。
例: if(アシスト力/急に大きくなる) アシスト機能/利用者が慣れないと感じる

参考：EARSパターン

	邦訳	要求の内容	時間関連
Ubiquitous	常時実行型	いつでも、どこでも、無条件に行うべき要求	
WHEN	事象応答型	特定の事象が発生したときにする応答	○
IF-THEN	問題対処型	特定の問題が存在するときにする対処	
WHILE	状態駆動型	特定の状態にある間にする処理	○
WHERE	環境依存型	特定の機能が使えるときに行うべき要求	
Complex	複合型	複合的な要求	

EARS:Easy Approach to Requirements Syntax

制御システムに関する要求を記述するために、ロールスロイス社が提唱している

電動アシスト自転車に関する記述例-1

対象システム：仮想的な電動アシスト自転車の開発

赤字：意図

青字：要求

1.開発計画
1,1　納期
1.1.1　発売時期
　新年度セールスの目玉/本製品にする
(:　要求
　販売開始時期/3月後半とする
1.2　コスト
1.2.1　販売価格
　購入可否/主婦が一人で判断できる
(:　要求
　販売価格/10万円未満とする
1.3　品質を検査する手段
1.4　安全を検査する手段
2.開発目的
2.1　達成目標
2.1.1　競争優位
　ブランド地位/トップ状態に維持する
(:　要求
　連続アシスト距離/40kmとする
(:　業界最高水準を達成すれば、ブランド地位を維持できる

電動アシスト自転車に関する記述例-2

2.2 システムに対する要求・制約
2.2.1 機能の利点
乗り心地/自然で滑らかにする
乗り心地/坂道でもパワフルで滑らかにする
(: アシスト基準
while(走行速度/時速10km以下) アシスト力/ペダルを踏む力1に対して
最大で2まで
while(走行速度/時速10km超で24km未満) アシスト力/順次弱める
while(走行速度/時速24km以上) アシスト力/ゼロ
(: SPEC3制御
while(変速位置/1速) アシスト力/時速10kmの手前で弱め始め、
24kmの手前で止める
while(変速位置/2速) アシスト力/時速24kmの手前で止める
while(変速位置/3速) アシスト力/基準どおり
(: 走行モード
while(走行モード/強モードにある) アシスト力/標準モードより強い
when(電源/オンになる) 走行モード/標準モード

対象システム:仮想的な電動アシスト自転車の開発
赤字:意図
青字:要求

意図体系テンプレート

1.開発計画
1,1 納期
1.1.1 発売時期
1.2 コスト
1.2.1 販売価格
1.3 品質を検査する手段
1.4 安全を検査する手段
2.開発目的
2.1 達成目標
2.1.1 競争優位
2.2 システムに対する要求・制約
2.2.1 機能の利点
2.3 使用者に対する要求・制約
2.3.1 使用目的
2.4 使用環境に関する仮定事項
2.4.1 法的制約
2.5 事故に関する情報
2.5.1 多発事故
2.6 ハザードに関する情報
2.6.1 急加速
2.6.2 重量
3.システム機能
3.1 製品に関する物理原則
3.1.1 変速機
3.1.2 前照灯
3.1.3 トリプルセンサー
3.1.4 バッテリー
3.1.5 自己診断
4.システム構造
4.1 安全関連系
4.2 新規と流用の区分
4.2.1 外部調達
5.システム運用
5.1 推奨する使用法
5.1.1 不慣れ事故
5.2 誤使用
5.2.1 不用意な使用
5.3 保守
5.3.1 定期検査

3階層目が意図項目

意図・要求の記述(一部)

**意図は、実現可能性などの要求特性を満たす必要がない。
それでいて、つい、要求を書いてしまう。
しかし、意図は、要求を縛る。**

2.開発目的
2.1　達成目標
2.1.1　競争優位
　ブランド地位/トップ状態に維持する
(:　要求
　連続アシスト距離/40kmとする

要求は、実現可能性、検証可能性などの要求特性を満たさなければならない。

(:　業界最高水準を達成すれば、ブランド地位を維持できる

意図を実現できるという論証も必要になる。

考察

- 要求分析段階で安全性を検証し、安全を作り込むためには、意図の体系的な記述が役に立つと考える。
- 意図を体系的に記述するときには、意図体系テンプレートに沿った記述が便利であり、その元になる標準的なフレームワークの整備が望まれる。
- 意図は、要求とは異なり、要求特性に制約されないが、要求の目的や根拠などの役割を担い、その記述には訓練、演習が必要だ。
- SSQLは簡潔な意図記述構文を提供し、仕様記述ツールSLPとの連携を可能としているので、要求の仕様化の現場で使えるのではないか。事例研究の継続が必要だ。

参考資料

- Engineering a safer world、N.Leveson著
- 平成26年度成果報告書「要求の仕様化に関する課題、プロセス及び手法」、JASAホームページ
- 日経テクノロジーオンライン、「意図を記述すれば、安全性が高まる」
- ET2016　JASA技術本部セミナー、「安全誘導型設計の特徴と試行」

2017年度活動計画概要

◆ 目的
- 安全が関わる要求を仕様化するプロセスの研究
- その仕様化を支援する方法論(プロセスモデル又は手法)の提案

◆ 方針
- 重点課題を共有し、自主的に活動し、相互啓発を図る。
- IPA/SECの関連WG等との連携を図る。

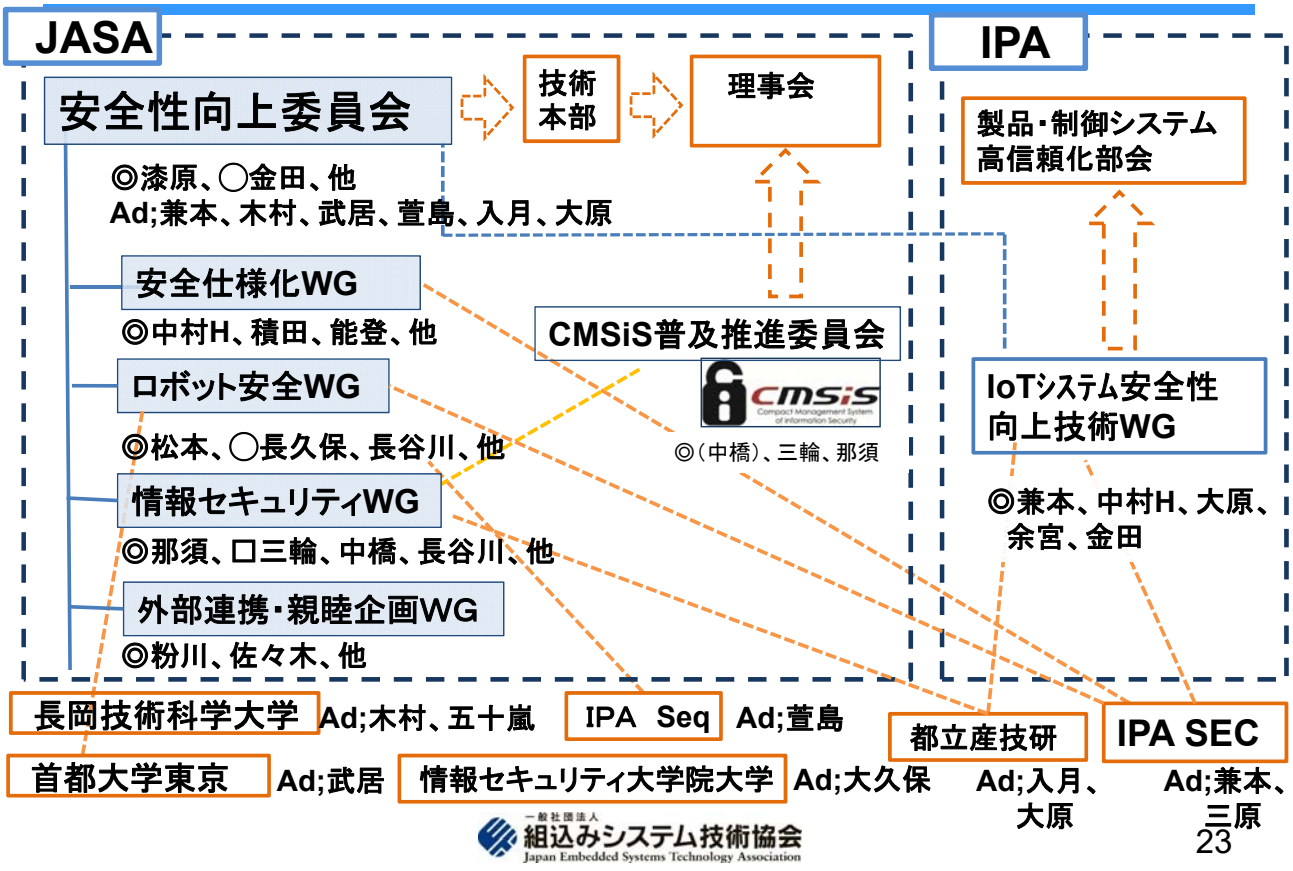
◆ 重点課題
- 安全誘導型設計を支援する手法及びツール
- 特に、STAMP/STPA、FRAM、SSQL

◆ 題材
- 電動アシスト自転車(メーカとの交流、連携を含む)
- ロボット安全WGの題材(交流、連携を図る)

◆ 活動方法
- 月1回の会合で活動成果を報告・討議する。
- 常時、メールを利用して情報・意見交換を進める。
- 適宜、勉強会を計画する。

安全性向上委員会:体制図

2017/4/21 R3



一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

◎;委員長、WG主査 ○;副委員長、副主査 口;技術顧問 Ad;外部アドバイザー

【意図記述言語SSQLの狙いと特徴～安全誘導型設計における意図記述手法～】

2017/7/12 発行

発行者 一般社団法人 組込みシステム技術協会
東京都中央区日本橋大伝馬町6-7
TEL: 03(5643)0211 FAX: 03(5643)0212
URL: http://www.jasa.or.jp/