開発要件の完成度を高めるアプローチの検討

2015年11月18日

JASA安全性向上委員会 SSQ-WG
貝瀬康利

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

前提となる用語

■ 本資料では、用語の定義を以下のように用いることにする。
- 一般的な意味ではなく、あくまで本資料における使い方として
- ただし、文献等からの引用に関しては、この限りではない.

■ 要求
- 実現したい事を利用者の言葉で述べたもの（発注視点）

■ 要件
- 要求を実現する人の言葉で述べたもの（受注視点）

アジェンダ

- 概念
  - 問題とソリューション
  - 要求と仕様
- 課題
  - 要件定義にまつわる課題
  - 事故事例
- プロセス
  - 工学的な基本プロセス
  - 各プロセスの課題とアプローチ
  - 分析視点として軽視できない特性
- アプローチ
  - 考え方
  - 取り組み紹介（模擬化学プラント）
    - 構成図／初期要件／初期の図／分析と検討／リファイン
- まとめ
  - 実施した内容の整理
  - 今後へ向けて

概念

課題

プロセス

アプローチ

まとめ

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

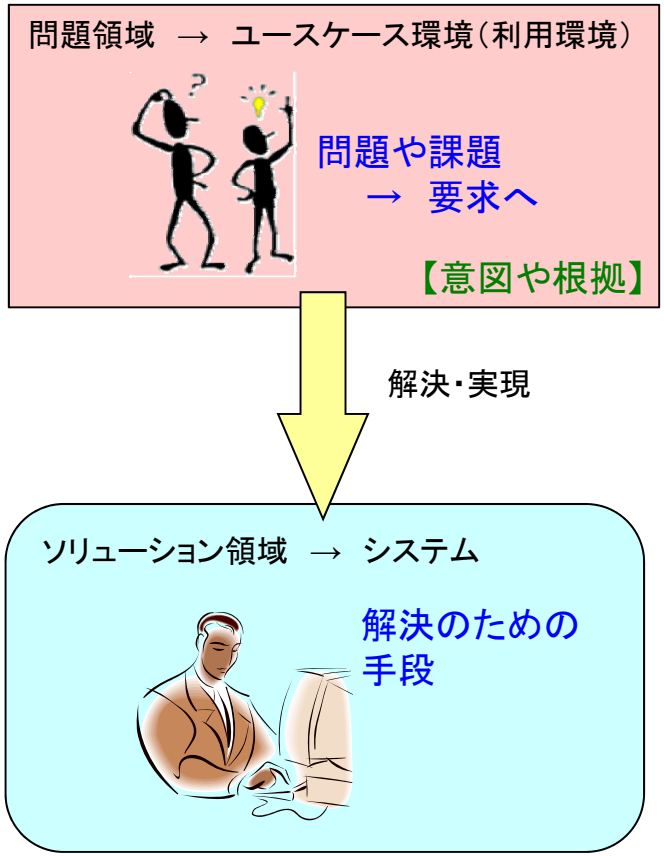
概念　＜問題とソリューション＞

■　問題領域とソリューション領域

- システムとは何でしょうか？
- なぜシステムを開発するのでしょうか？

- 人が生活したり、生きていく上では様々な問題や課題に直面します。
  - 自然な流れとして、そうした課題を解決するためにどうすれば良いか、実現したいことを考え始めます。
  - そして実現され、提供されるものは、問題領域にヒットするものでなければ無用の長物になってしまいます。

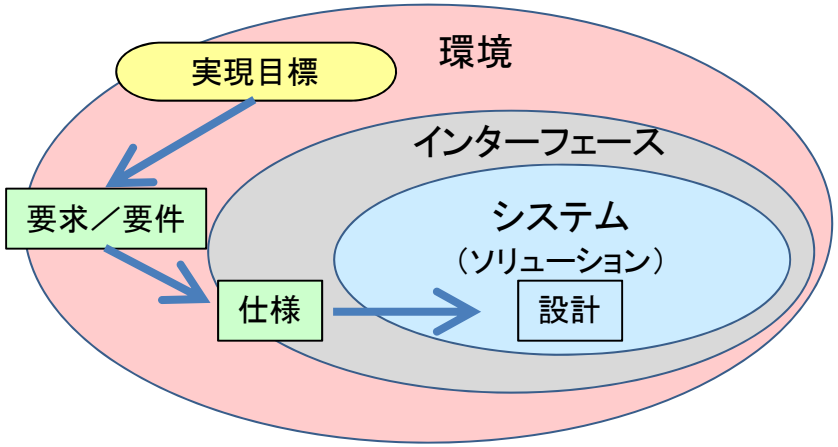
要求とか仕様とかを理解するには、こういったことを原点に立ち返って、よく考える必要があります。



概念　＜要求と仕様＞

■　要求／要件
- システムを利用することによって実現したいこと
  - 利用環境から見た、システムとしての実現目標
  - 目的と手段を混同しないよう、利用環境の言葉で記載

■　仕様
- システムが利用環境に対して必要な機能を提供するための境界条件
  - システムと利用環境の接点である
  - ソリューション（手段）を含めた言葉で記述される



整理すると……

問題提起の視点で述べたものが要求、
問題解決の視点で述べたものが仕様

概念

課題

プロセス

アプローチ

まとめ

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

課題　＜要件定義にまつわる課題＞

カテゴリ	事業戦略・事業計画	システム化の方向性	システム化計画	要件定義
事業戦略・計画とシステム化の乖離	12	10		
対応すべき課題の優先順位が曖昧	8		2	
ユーザニズの把握不足	5			
組織体制、役割分担が不明確	4	10	13	13
商品、サービスの検討不足		9	3	
プロジェクトの目的が不明確		7	3	4
契約、見積が不十分		3	13	3
業務知識、経験スキルの不足		3	6	7
組織ビジョンが不明確		2		
既存システムの仕様が不明確		1	1	
新技術、サービスの採用		1		
開発方針、計画が不十分			7	
プロジェクト管理が不十分			3	
費用対効果が不明確			3	
要件定義不足、レベルの甘さ				26
要件定義の終了条件が曖昧				6
リスク管理の甘さ				1
計	29	46	54	60

（出典） IPA 「高品質のための上流工程における企業の課題・取り組み事例集」

システムの品質問題の原因

社内の開発体制に問題	13.90%
ベンダーの選択に問題	10.60%
要件定義が不十分	35.90%
システムの企画が不十分	18.70%
システムの設計が不正確	19.10%
システムの開発作業の質が悪い	13.10%
テストが不十分・移行作業に問題	21.90%
エンドユーザへの教育が不十分	19.10%
運用計画が利用形態に沿っていない	7.50%
その他	27.70%
（有効回答　498件）	

（出典） 日経コンピュータ　2003.11

- 要件定義の甘さは課題領域としての比重が大きい.
- 要件定義の課題は、一般に以下のような言葉で表される.
  - 完全性、一貫性、明確性、追跡性、検証可能性、正確性
- 要件定義は、安全上も重要.
  - ソフトウェアが関与した事故の大多数は要件の欠陥に遡る（「セーフウェア」15章）

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

課題

＜事故事例＞

- アリアン5の打ち上げ事故
- 事象
  - 1996年6月4日、ESA（※）によって打ち上げられたアリアン501型ロケットが、打ち上げ後40秒程度で爆発した。これはアリアン5として初の打ち上げであった。
- 全経済損失
  - 開発費含めて、80億ドル[USドル]
- 直接要因

ソフトウェアのエラー：
加速度を扱う変数のオーバーフロー

- 根本原因

アリアン4にて使用実績のあるソフトウェアが再利用されたが、アリアン5では、旧式では考えられない巨大な加速度が発生したため、そこを扱う変数のオーバーフローが発生した。つまり再利用時の要件の検討不足であった。

該当箇所の詳細要件の再利用性も再検討すべきであった

※ Image credit: ESA/Arianespace

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

概念

課題

プロセス

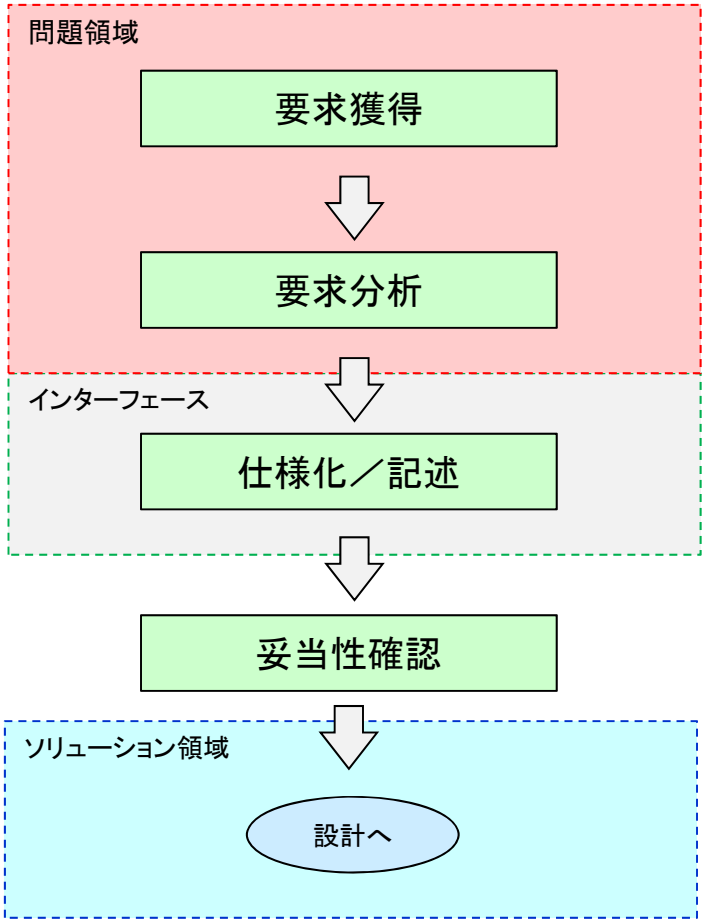
アプローチ

まとめ

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

プロセス　＜工学的な基本プロセス＞

■　4つの基本プロセス　※



実現したいことを、問題領域の言葉で記述.

素人による要求を分析し、システムとしての成立性要求から仕様への論理的な筋道を作成する.

要件を実現するための手段を「仕様」として表現する.

一貫性や網羅性、追跡性などの妥当性を確認する.

それぞれの目的や課題に応じた方法を検討する事が重要

仕様に基づき、信頼性に留意して作りこみを行う

※参考文献 「要求定義書・要求仕様書の作り方」 山本修一郎　著

プロセス　＜課題とアプローチ＞

問題領域

プロセス	課題	開発の注意点	手法のアプローチ
要求獲得	①曖昧で具体性や正確性に欠ける ②要求の変動性がある ③要求を出す側が気づかない隠れた要求もある	・要求の網羅性に注意	要求を得る＞ マインドマップ、ユースケース／ステークホルダ分析、ガイドワードレビュー 要求を記述する＞ EARS、SLP ▸ 自然言語 → 構文化
要求分析	①獲得された要求は、定量化や体系化が難しく、柔軟性の高い分析法が求められる。 ②上記に対処する手法が確立されておらず、開発側が要求の矛盾や偏りに気づけないことが多い	・重視する特性(一貫性や追跡性)は何か? → 分析視点としての特性による完成度向上	要求を分析＞ 要求図（SysML）、GSN、USDM ▸ 半形式 → 構造化
仕様化／記述	①仕様化の記法や手法は多岐にわたり選択が難しい。 ②最適な手法ではなく、開発者がやり易い方法が選択される場合が多い	・仕様のモデル化 → 概念モデル ・特性の洗練・強化	要件から仕様を具体化＞ SysML/UML、VDM、Z、、、 ▸ 半形式 → モデル化（構造／振る舞い） ▸ 形式 → 形式化（動作／モデル検査）
妥当性確認	①判断基準の定量化が難しく、定性的な判断となる ②上記理由で判断が属人化し易い	・クライテリアとして特性を用いる	特性をチェック＞ チェックリスト、レビュー

過去の失敗の多くは、問題領域、特に「要求分析の甘さ」に原因があると考えた

プロセス　＜分析視点＞

■　分析視点の「例」

特性	意味付けの例	根拠
安全性	ASIL-Bに準拠し、不合理なリスクが存在しないこと	
シンプルさ （対 複雑性）	システムコンテキストの構造明確化と構成要素間における相互作用の見通しが立って、影響範囲が限定できる	
追跡性	全ての仕様は、最上位の要求まで遡れること. （要求に対応しない仕様は冗長な仕様となる）	
要求の完全性	必要な要求がすべて網羅（抽出）されている.	
要求/要件の一貫性	抽出された要求/要件を統括して矛盾が含まれない.	
要求の必要性	すべての要求の根拠が明確になっている.（根拠が不明確な要求を扱わない）	
要求/要件の非冗長性	互いに重複する内容が混在していない.	
仕様の完全性	全ての要求が仕様化されている.（仕様化されない要求がない）	
仕様の一貫性	仕様と利用環境、システムとの間に矛盾が存在しない	
仕様の正確性	仕様に曖昧さがなく、上位から繋がる要求/要件を正しく具体化している.（ex. アリアン5の事例）	
仕様の検証可能性	仕様が意図した通りに実現できたかどうか確認する手段が具体化できる.	
変更容易性	影響範囲が限られる、または、明確。 → 追加／変更／削除が容易	

分析視点を掘れさせない

一般的な分析視点に加えて、ドメイン固有の視点を整理・定義し、根拠を明記

例えば

①過去に問題となった要因
②製品の性質上重視すべき特性（安全性など）

概念

課題

プロセス

アプローチ

まとめ

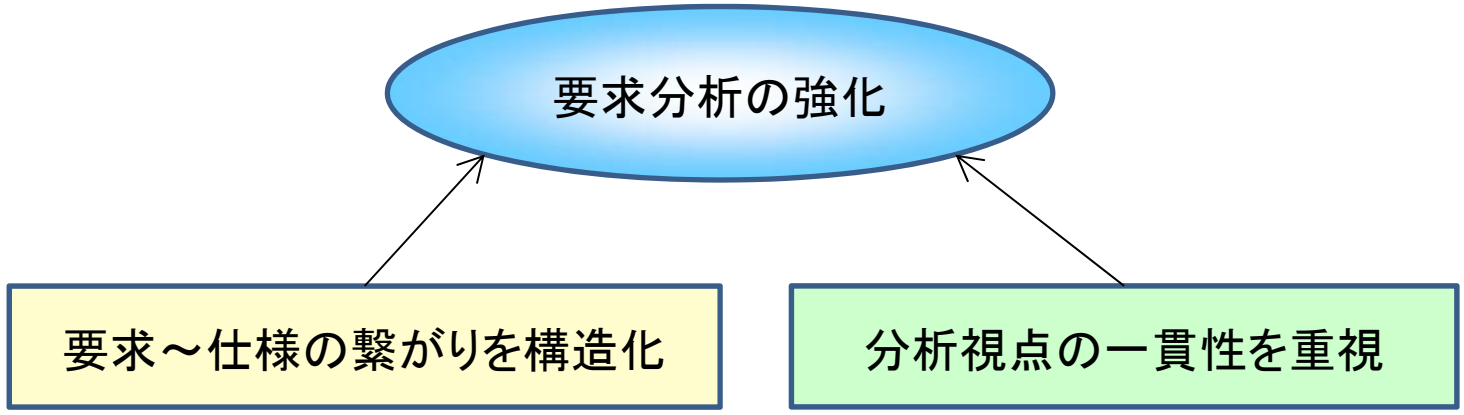
一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

アプローチ　＜考え方＞

■　要求分析を強化
- 要件定義の甘さは、課題としての比重が大きい
- 事故や不具合の要因は、問題領域(要求)の分析の甘さにある

■　仕様への繋がりを構造化
- 要求～要件～仕様　の繋がりを重視
  - 問題領域からソリューション領域への論理的な筋道の明確化
- 曖昧さが残る上流領域は、形式的な枠に囚われない柔軟性も必要
  - まずは各項目を階層化してみた.

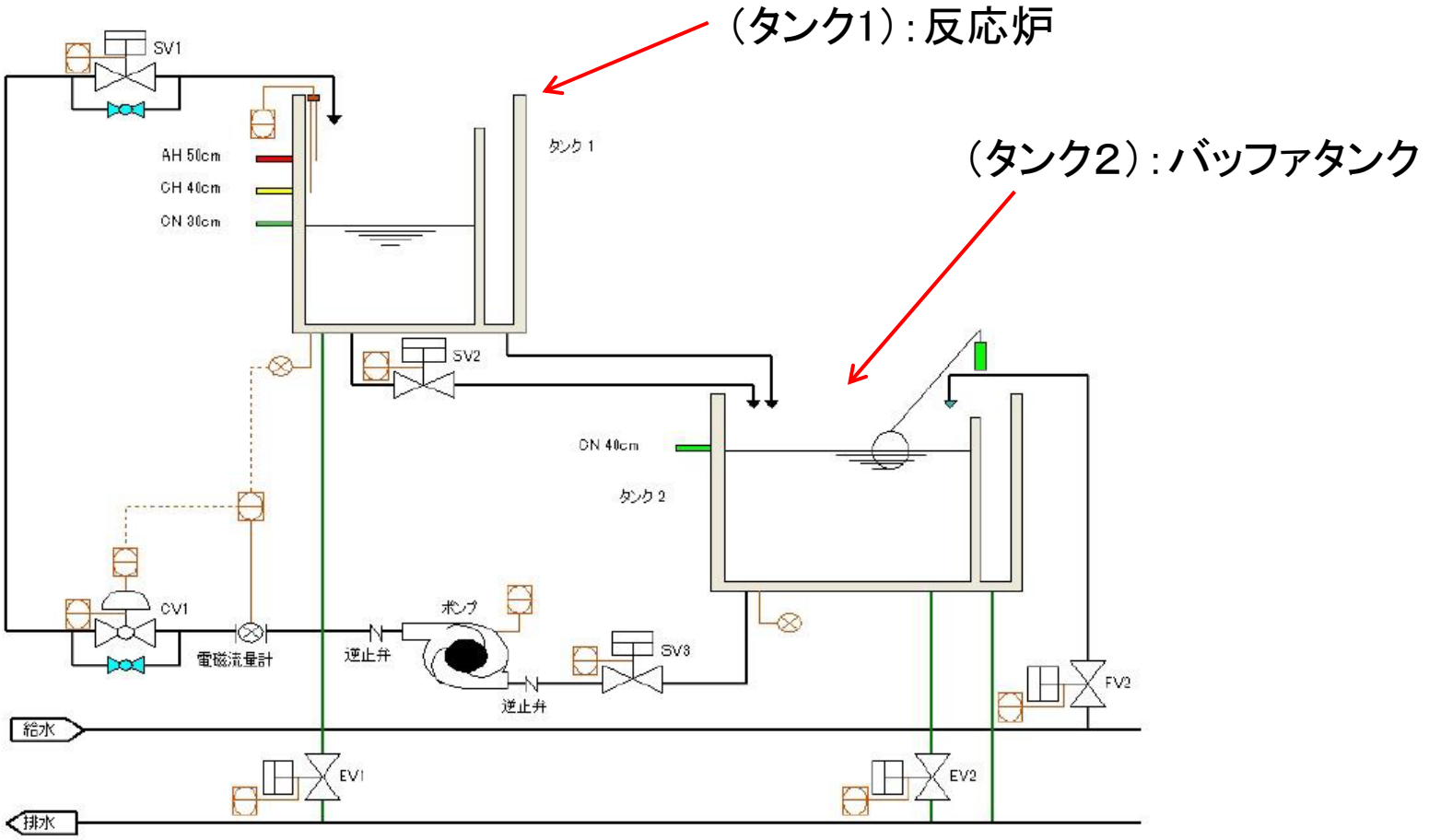
■　分析視点の一貫性を重視
- ブレない視点を初期に固める



アプローチ

<取り組み紹介：題材>

■ 模擬化学プラントの構成図



出典 「大規模・複雑化した組込みシステムのための障害診断手法」
～モデルベースアプローチによる事後V&Vの提案～

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

アプローチ

＜初期の記述内容＞

■ 機能要求として書かれていたこと…

- REQ1
  - タンク1を反応炉と想定し、その水位が一定の目標値になるように制御する。
- REQ2
  - タンク2はバッファータンクとし、タンク1への給水用の水を一旦保管するために用い、また、タンク1からの排水を受けるために用いる。
- REQ3
  - タンク2の水位が低下した場合はフロート弁で自動注水するが、排水機能は持たない。
- REQ4（安全要求）
  - タンク1の水位がアラートレベル(40cm)を超えた場合、自動的または運転員の手動要求でドレン配管の排水弁を開いて排水する。その際、ドレン配管からの排水速度は、ポンプの最大容量での注水速度を上回るよう設計する。

■ 安全制約

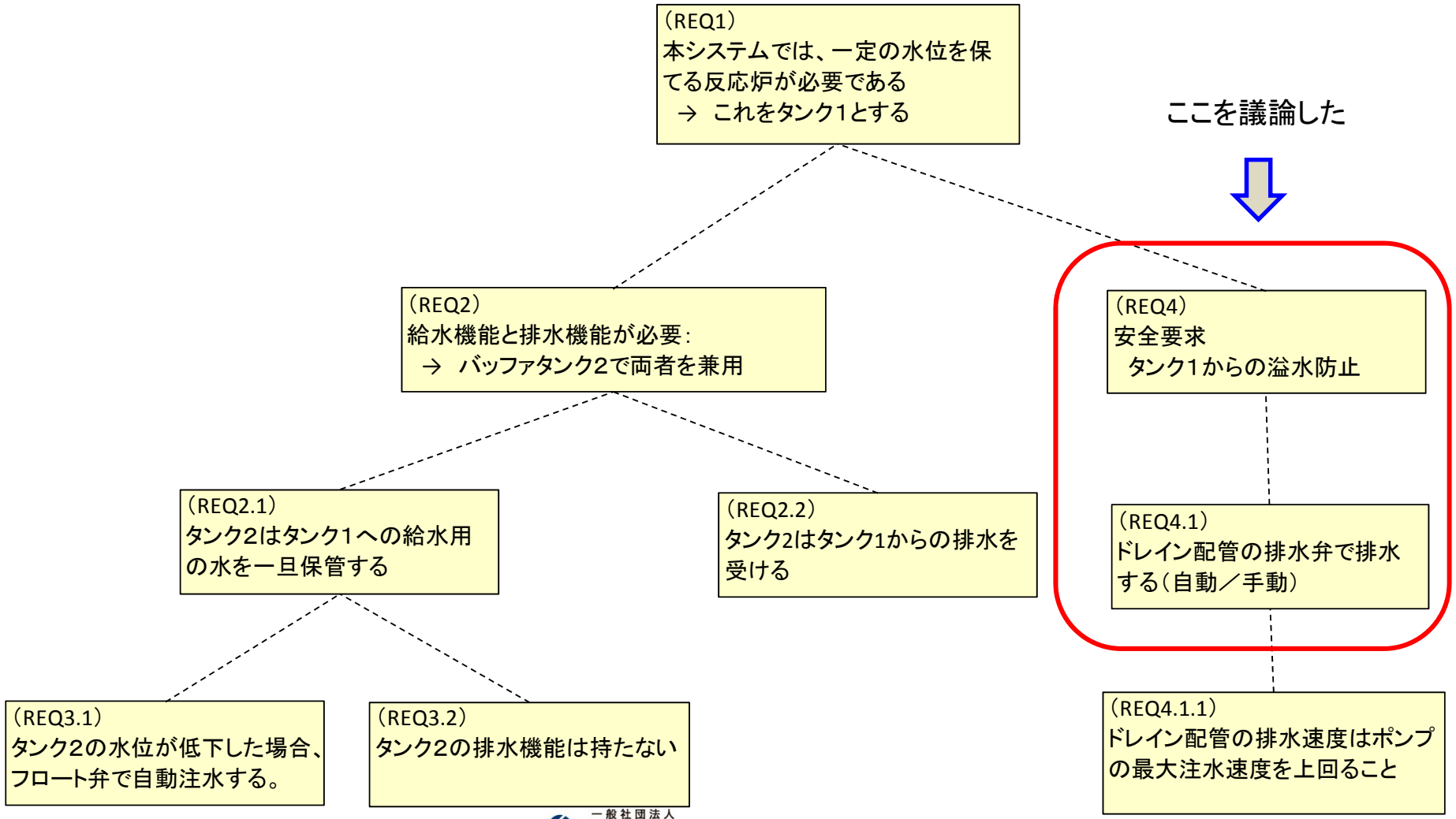
- プラントのハザードとして、タンク1ならびにタンク2の溢水を仮定し、タンク1からの溢水防止を安全制約とする。配管からのリークは、インシデント（軽微故障）扱いである。

■ これらを見て思ったこと

- 個別の機能要求の階層とか繋がりがわからない。
- ひとつの項目に複数の要素が入っている

アプローチ ＜図化＞

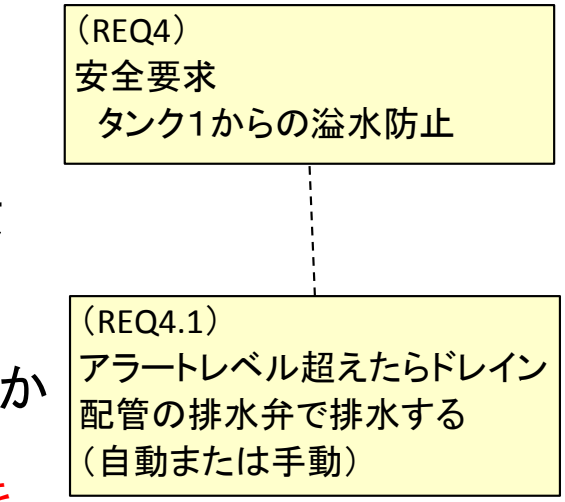
■ まずは、記載内容を図にしてみた
- 論理的な繋がりと階層



アプローチ　＜図の議論・検討＞

■ 図の繋がりを安全視点で議論・検討した
- 安全要求に基づき、フェールセーフを検討
- 抜けていることが見えてきた

■ 検討結果として見えてきたこと
- 排水以前に、溢水防止の目的からして、 まず水位の監視が必要だろう
  - ①水位監視　②排水
- 手動が必要な根拠は、自動制御が上手く働かない場合を想定している・・・
  - 自動運転による水位制御にて、手動での制御を自動運転より高い優先度に置く設計が必要
  - フェールセーフ視点から、(排水のみでなく)水位監視もカメラなど設置し、人の目で判断できるように設計すべき。
- 災害時の想定も必要
  - 電気系統が死んでも、人手で排水できること
    - ✓ 人力でバルブを開けられないような設計はNG

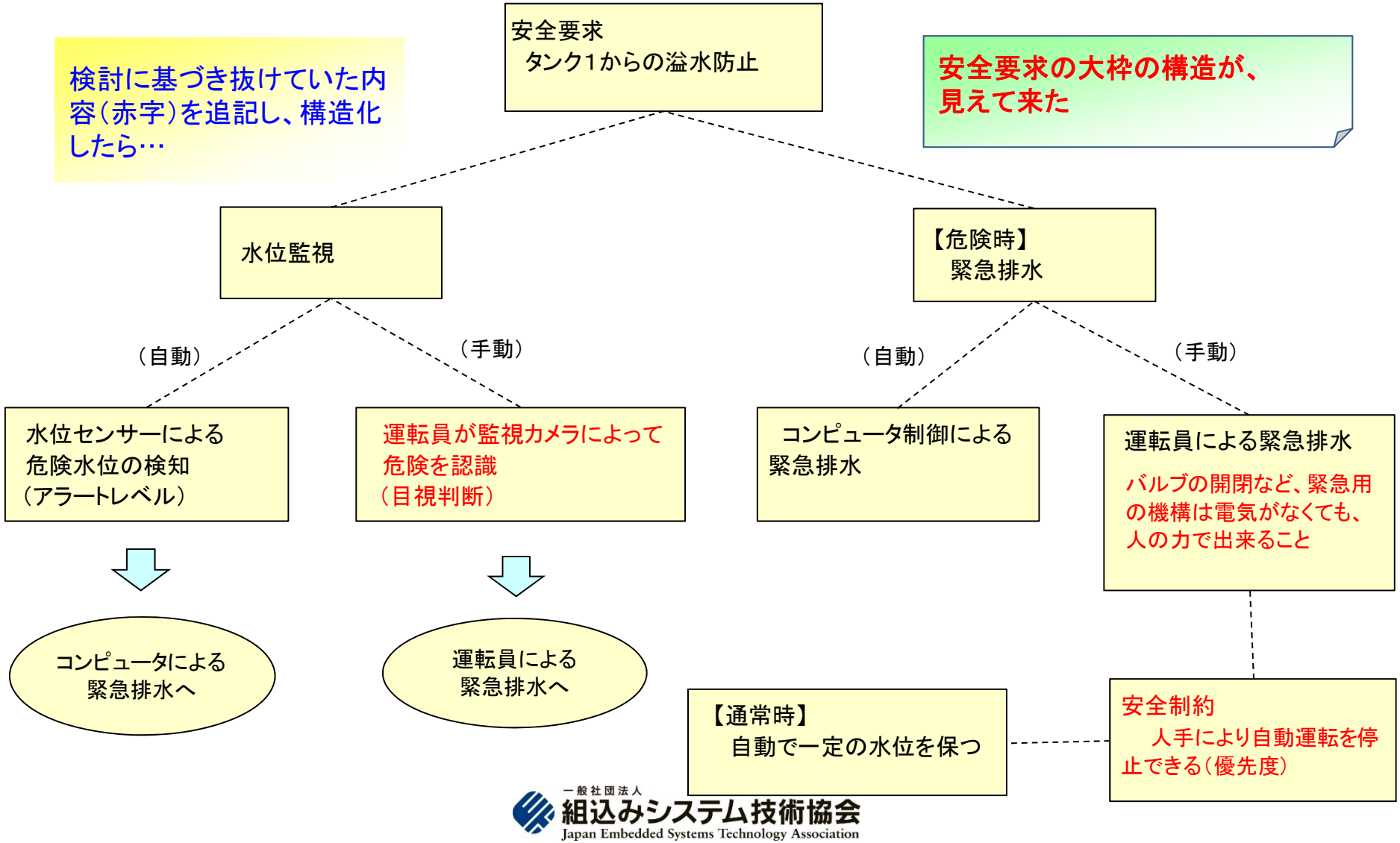


アプローチ

＜図のリファイン＞

■　図をリファイン（安全要求）

検討に基づき抜けていた内容（赤字）を追記し、構造化したら…



概念

課題

プロセス

アプローチ

まとめ

まとめ

■　実施した流れ

流れ	No.	実施項目 または チェックポイント
分析視点の決定	1	仕様として重視する分析の視点を決定し、共有・合意する
構造化	2	収集された要求の一覧を作成する
	3	上記の要求に階層を付けてまずは、図化してみる
	4	上記の要求項目を要素に分解し、図をリファインする
	5	機能としての抜け漏れがないかを議論・検討する その際、階層を上から下にたどりつつ、論理的な筋道の根拠や妥当性を議論する
安全性	6	安全目標を達成するために必要な機能が網羅されているかを検討する
	7	要求/要件の構造を議論し、フェールセーフの検討が十分かを洗い出す。 ①制御が意図した通りに動作しない場合、どう制御すべきか？ ②その場合、安全目標を阻害するすべての要因を抑止できる構成となっているのか？ 例えば… ・全電源喪失 → 人力で排水できるように機械的に設計されているか？ ・自動運転のエラー → 手動で抑止できるか？
	8	フェールセーフの視点から、運用される制御の優位性は以下のように設計する 人間 ＞ 機械 ＞ コンピュータ

まとめ

■ 効果について

- 要求分析に狙いを定めた今回のアプローチによって、要件の完成度を上げる効果が期待できそうである

■ 今後の課題

- 要求分析における視点を決定の上、その構造化を行うためのノウハウの具体化・標準化がキーである

参考文献

- 「要求定義書・要求仕様書の作り方」
  - 山本修一郎
- 「ソフトウェアの要求発明学」
  - スザンヌ・ロバートソン／ジェームズ・ロバートソン　河野正幸（訳）
- 「ソフトウェア要求　顧客が望むシステムとは」
  - KarlE.Wiegers著　渡部洋子（監訳）
- 「ソフトウェア要求と仕様　実践、原理、偏見の辞典」
  - マイケル・ジャクソン　玉井哲雄／酒匂寛（訳）
- 「ソフトウェア要求管理　新世代の統一アプローチ」
  - ディーン・レフィングウェル／ドン・ウィドリグ　石塚圭樹　他（訳）
- 「システムズモデリング言語SysML」
  - サンフォード　フリーデンタール、アラン ムーア、リック スタイナー　西村秀和　他(訳)
- 「SysML/UMLによるシステムエンジニアリング入門」
  - Tim・Weilkiens　今関剛／貝瀬康利（監訳・訳）

参考資料(WEB)

- 大規模・複雑化した組込みシステムのための障害診断手法
  - https://www.ipa.go.jp/sec/reports/20150331_2.html
- 要求分析ツリー
  - http://itpro.nikkeibp.co.jp/article/Watcher/20071009/283860/
- 要求の構造化
  - http://businesmethod.blog.jp/archives/1019237331.html
- 要求開発アライアンス
  - http://www.openthology.org/index.html
- あの事故はなぜ起きたのか？
  - http://www.kumikomi.net/archives/2008/12/33safe1.php?page=4

以上、ご静聴ありがとうございました.

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

「開発要件の完成度を高めるアプローチの検討」

2015/11/18 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/TOP/

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