トップエスイー修了制作

ソフトウェア開発における欠陥分析と HAZOP のガイドワードを用いたリスク観点導出の方法

フェリカネットワークス株式会社　増田 礼子　Ayako.Masuda@FeliCaNetworks.co.jp

研究の背景と課題

組み込みソフトウェア開発の最終段階において，プロジェクトメンバにインタビュー実施した結果，自分たちがレビューやテストを十分に行えているか確信が持てない開発者が多かった．開発者が抱く漠然とした不安感を払拭するために，**開発の初期段階でリスクを漏れなく洗い出す**方法を検討，提案したいと考えた．

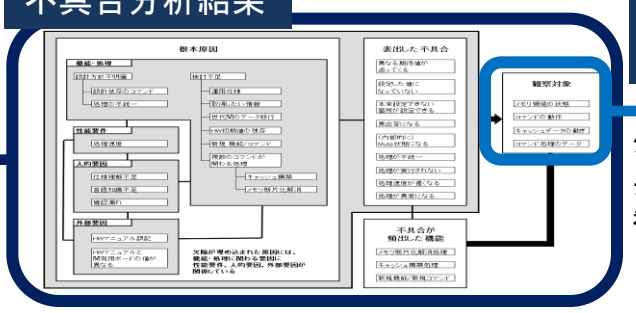
HAZOP ガイドワードを利用した解決

①実プロジェクトで発生した不具合を分類し，欠陥が埋め込まれた根本原因を分析する．
②分析結果に対し，化学プラントの安全性を評価するために開発された HAZOP の考え方を応用した先行研究結果を参考にし，その流用可能性の検証を行いながら，対象ドメイン向けのリスク観点を導出するためのガイドワードを検討，提案する．

検討モデル

①不具合分析の結果を基に，**「ガイドワードと発生した不具合との関係表」**の作成と**「観察対象ごとのガイドワード集」**の検討を並行して行うことにより，ガイドワードの検討および妥当性の検証を行った．表出した不具合の範囲では矛盾していないことから，ガイドワードは妥当であると判断した．

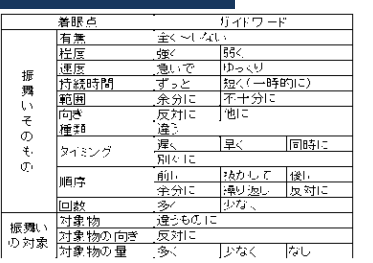
不具合分析結果



仕様策定におけるガイドワード

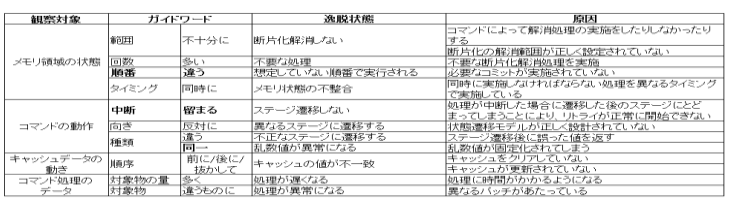
(河野哲也，ソフトウェア要求仕様における HAZOP を応用したリスク項目設計法)

外側から見える共通の事象を観察対象とした



着眼点		ガイドワード		
振舞いそのもの	有無	全くしない		
	粒度	強く	弱く	
	速度	急いで	ゆっくり	
	持続時間	ずっと	短く(一時的に)	
	範囲	余分に	不十分に	
	向き	反対に	他に	
	種類	違う		
	タイミング	遅く	早く	同時に
		別々に		
	順序	前に	抜かして	後に
		余分に	繰り返し	反対に
	回数	多く	少なく	
振舞いの対象	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	なし

妥当性の検証 ①



観察対象	ガイドワード		逸脱状態	原因
メモリ領域の状態	範囲	不十分に	断片化解消しない	コマンドによって解消処理の実施をしたりしなかったりする
				断片化の解消範囲が正しく設定されていない
	回数	多い	不要な断片化解消処理を実施	
	順番	**違う**	想定していない順番で実行される	必要なコミットが実施されていない
	タイミング	同時に	メモリ状態の不整合	同時に実施しなければならない処理を異なるタイミングで実施している
コマンドの動作	**中断**	**留まる**	ステージ遷移しない	処理が中断した場合に遷移した後のステージにとどまってしまうことにより，リトライが正常に開始できない
	向き	反対に	異なるステージに遷移する	状態遷移モデルが正しく設計されていない
	種類	違う	不正なステージに遷移する	ステージ遷移後に誤った値を返す
キャッシュデータの動き	順序	前に／後に／抜かして	キャッシュの値が不一致	乱数値が固定化されてしまう
				キャッシュをクリアしていない
コマンド処理のデータ	対象物の量	多く	処理が遅くなる	キャッシュが更新されていない
	対象物	違うものに	処理が異常になる	処理に時間がかかるようになる
				異なるバッチがあたっている

ガイドワードと発生した不具合との関係表

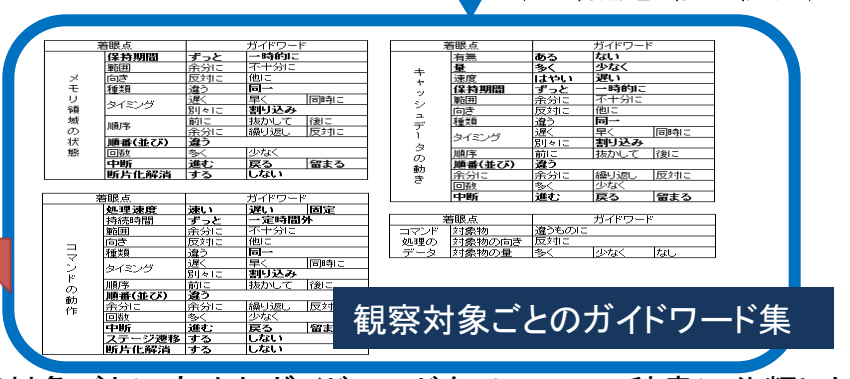
ガイドワード集を集約した辞書

着眼点		ガイドワード			観察対象のカテゴリ			
					状態	動作	動き	データ
観察対象	有無	**ある**	**ない**				○	
	量	**多く**	**少なく**				○	
	程度	強く	弱く					
	速度	**はやい**	**遅い**				○	
	処理速度	**速い**	**遅い**	**固定**		○		
	持続時間	ずっと	**一定時間外**			○		
	保持期間	**ずっと**	**一時的に**		○		○	
	範囲	余分に	不十分に		○	○	○	
	向き	反対に	他に		○	○	○	
	種類	違う	**同一**		○	○	○	
	タイミング	遅く	早く	同時に	○	○	○	
		別々に	**割り込み**					
	順序	前に	抜かして	後に	○	○	○	
		余分に	繰り返し	反対に				
	順番(並び)	**違う**			○	○	○	
	回数	多く	少なく		○	○	○	
	中断	**進む**	**戻る**	**留まる**	○	○	○	
	対象物	違うものに						○
	対象物の向き	反対に						○
	対象物の量	多く	少なく	なし				○

観察対象のカテゴリ	
カテゴリ	状態
	動作
	動き
	データ

着眼点		ガイドワード		
観察対象	BT	進む	戻る	留まる
	断片化解消	する	しない	
	ステージ遷移	する	しない	

妥当性の検証 ②



着眼点		ガイドワード			
メモリ領域の状態	**保持期間**	**ずっと**	**一時的に**		
	範囲	余分に	不十分に		
	向き	反対に	他に		
	種類	違う	**同一**		
	タイミング	遅く	早く	同時に	
		別々に	**割り込み**		
	順序	前に	抜かして	後に	
	順番(並び)	**違う**			
	回数	多く	少なく		
	中断	**進む**	**戻る**	**留まる**	
	断片化解消	する	**しない**		

着眼点		ガイドワード			
キャッシュデータの動き	有無	**ある**	**ない**		
	量	**多く**	**少なく**		
	速度	**はやい**	**遅い**		
	保持期間	**ずっと**	**一時的に**		
	範囲	余分に	不十分に		
	向き	反対に	他に		
	種類	違う	**同一**		
	タイミング	遅く	早く	同時に	
		別々に	**割り込み**		
	順序	前に	抜かして	後に	
	順番(並び)	**違う**			
	余分に	余分に	繰り返し	反対に	
	回数	多く	少なく		
	中断	**進む**	**戻る**	**留まる**	

着眼点		ガイドワード		
コマンド処理のデータ	有無	**ある**	**ない**	
	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	なし

観察対象ごとのガイドワード集

②観察対象ごとに定めたガイドワードを以下2つの辞書に分類した．
- **対象ドメインにおけるガイドワード辞書**
- **組み込み設計におけるガイドワード辞書**

加えて，**観察対象となるカテゴリ**をリスト化し，カテゴリごとに必要となった着眼点を辞書に追加した．

結論

- HAZOP のガイドワードを利用してリスクを検討することにより，組み込みソフトウェア開発における，網羅的なリスク観点の抽出・検討が可能となる．
- 欠陥分析の結果をドメインの特性とし，その特性に基づいてガイドワードを選定・利用することにより，ドメイン固有のリスクの低減が可能となる．

今後の展望

- 頻出する，または，リスク観点として重要なガイドワードを派生開発や次期開発で用いる．
- 仕様の策定やテスト観点の検討など，上流工程での活動においても有用なリスク観点の抽出を行う．
- 対象ドメインに対するガイドワードの辞書を拡張し，利用していく．
- さらに，組み込みシステムにおけるガイドワードの辞書をまとめていきたい．

NII 国立情報学研究所 National Institute of Informatics
トップエスイー ～サイエンスによる知的のものづくり教育プログラム～