



Engineering for a Safer Tomorrow

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

車載半導体・センサ向け 機能安全開発支援

要求・Safety Architecture・Safety Mechanism・検証方針を具体化し、
Safety Analysis／RTL Verification／Fault Injectionまで一貫して支援



Functional
Safety



ASIC / Sensor
Design



Verification



Safety
Analysis

ベリフィケーションテクノロジー株式会社

ENGINEERING FOR A SAFER TOMORROW

1. ご提案の背景とPhase1の目的

開発初期における機能安全開発の課題

- ・開発初期段階では、HSRやSafety Mechanism等の仕様が固まり切っていない
 - ・一方で、外部委託では作業範囲・成果物・責任分界を明確にする必要がある
- 初期2～3か月を「Phase1」として区切り、要求・Safety Architecture・Safety Mechanism・検証方針等を具体化し、Phase2以降の作業範囲・成果物・工数を明確にする進め方をご提案します。

現在



製品仕様・HSR・安全機構が
検討段階



Phase1

(初期2～3か月)



要求・Safety Architecture・
Safety Mechanism・検証方針等
を具体化



Phase2以降



作業範囲・成果物・工数を
明確化して個別発注

Phase1の目的

Phase2以降を「成果物を明確にした委託」として発注可能な状態にする

2. Phase1における検討・具体化範囲

STEP 1



製品・Safety要求理解

製品仕様／ASIL／SG・FSR・TSR・HSR／前提条件の理解

STEP 2



HSR具体化

HSRの妥当性・抜け漏れ・曖昧性確認、
および機能BlockへのAllocation

STEP 3



Safety Architecture

Safety Architectureの検討・提案
(故障検出／通知経路／Safe State／FTTI充足性 (FDTI+FRTI) の確認)

STEP 4



Safety Mechanism

Safety Mechanismの検討・提案
(ECC／Parity／CRC／Monitor／冗長化等)

STEP 5



Analysis / Verification計画

Safety Analysis／Verification計画の立案
(FMEA・FMEDA／RTL検証／Fault Injection等)

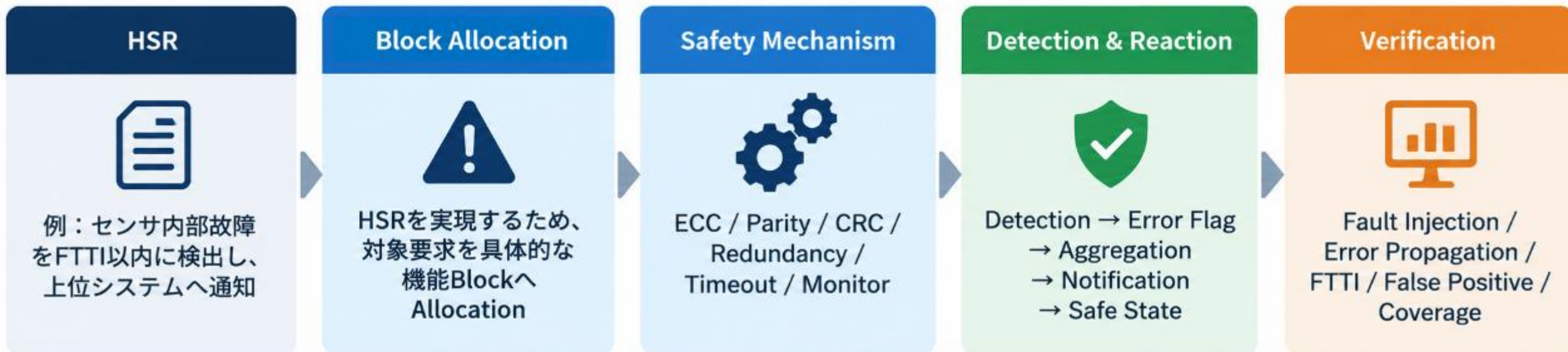


お客様：製品要求・設計思想・既存仕様
製品知識・市場要求・システム要件



Vtech：FuSa・ASIC設計・検証ノウハウ
機能安全・設計・検証の専門知識と実績

3. Safety Requirementから実装・検証への具体化



Vtechの支援ポイント

HSRのレビューに留まらず、Safety Mechanismの配置・実現方法から
RTL検証／Fault Injectionまで見据えて具体化

4. Phase1 実施スケジュール（想定2～3か月）

Week 1-3

Gate 1 (STEP1)
Safety Requirement



- 製品仕様理解
- SG / FSR / TSR / HSR確認
- 対象範囲・ASIL確認
- Safety Requirement課題整理



Customer Review → 合意

Week 4-7

Gate 2 (STEP2~STEP4)
Preliminary Safety Architecture



- HSR Allocation
- Preliminary Safety Architecture
- Safety Mechanism検討
- Safe State / FDTI / FRTI



Customer Review → 合意

Week 8-12

Gate 3 (STEP5)
Analysis & Verification



- Preliminary FMEA
- FMEDA方針
- Functional Safety Verification Plan (RTL / Fault Injection)
- Phase2 WBS・工数算出



Customer Review → 合意

各Gateで認識を合わせながら進めることで、
開発初期の仕様変動を吸収しつつ成果物を段階的に具体化

5. Phase1成果物とPhase2へのInput

Input		Safety Plan	お客様作成のSafety Plan等をInputとして確認
1		HSR Allocation	HSR → BlockへのAllocation／課題・前提条件整理
2		Preliminary Safety Architecture / Analysis	Safety Architecture / Error Propagation / Preliminary FMEA
3		Functional Safety Verification Plan	RTL Simulation / Fault Injection / FDTI・FRTI / False Positive / Coverage
4		Phase2 工数算出・実施計画	作業項目／成果物／必要工数／スケジュール



6. Phase1から量産開発までのVtech支援イメージ



Vtech 一貫支援範囲



Vtechは、機能安全文書作成だけでなく、センサ／ASIC設計・RTL検証の知見を活用し、Safety Mechanismの具体化から検証・Safety Analysisまで一貫して支援します。

7. Phase1モデルケース別 参考イメージ

	Case A：既存成果物あり	Case B：標準モデル	Case C：具体化支援大
 想定状態	既存成果物を活用し レビュー中心	一部検討中／共同具体化	未整備部分が多く Vtech支援大
 HSR	概ね整備済	一部検討中	未整備部分あり
 Safety Architecture	概ねあり	一部検討中	Vtechと共同具体化
 Safety Mechanism	概ね決定	一部検討済	Vtechから提案
 想定期間	約2か月	約2～3か月	約3か月
 参考費用	500～600万円程度	約720万円	900～1,000万円程度



※ 期間・費用は参考モデルです。正式見積は対象範囲、既存成果物の成熟度、対象Block数、成果物粒度等を確認後に算定します。

※ 上記はモデルケースに基づく概算です。実際の対象範囲、既存成果物の成熟度、対象Block数、Phase1成果物の内容・粒度等を確認のうえ、正式見積をご提示します。

見積算定にむけた確認事項

8. Phase1 作業範囲・見積算定に向けた確認事項

Phase1の具体的な作業範囲・成果物・必要工数を明確化するため、以下について確認させていただきます。

確認項目		主な確認内容	見積への影響
01		対象製品・開発範囲	対象規模
02		ASIL・Safety要求	要求分析
03		HSRの成熟度・件数	HSR
04		Safety Architecture	Architecture
05		Safety Mechanism	Mechanism
06		Safety Analysis	Analysis
07		Verification	Verification
08		Phase1成果物	成果物作成
09		開発スケジュール	体制・投入時期
10		レビュー・承認方法	PM/Review
11		インプット資料の準備	仕様理解・解説工数



確認後、Phase1の作業範囲・成果物を合意し、必要工数を積み上げた上で正式見積をご提示します。

※ Phase1の実施期間（想定2～3か月）とVtechリソース投入工数は同一ではなく、対象範囲・既存成果物の成熟度・成果物粒度に基づき工数を算定します。

開発支援ロードマップ

Phase2以降の開発支援ロードマップ

Phase1で要求・Safety Architecture・Safety Mechanism・検証方針を具体化し、Phase2以降は成果物単位で段階的に委託可能



Thank you!