2022 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION JAPAN

ISO26262対応LSI開発における回路規模・消費電力増の小さい機能安全アーキテクチャ

ベリフィケーションテクノロジー株式会社　濵谷敏行

accellera SYSTEMS INITIATIVE

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

概要

電子部品の“フォールト”や“エラー”による事故を抑制するために、車載向けLSIに対しては、ISO26262に準拠した設計を行うことが必須になっている。ISO26262に準拠するためには、自動車安全水準（ASIL）のレベルに応じた、安全機構の組込みが必要になる。

これらの安全機構の実装は、必然的に、回路規模や消費電力の増加を招く。ただ、LSIの各回路モジュールの利用用途を考慮した機能安全アーキテクチャとすることで、増加量の大きな抑制が可能となる。

本発表では、回路規模や消費電力の増加が少ない機能安全アーキテクチャの紹介を行う。

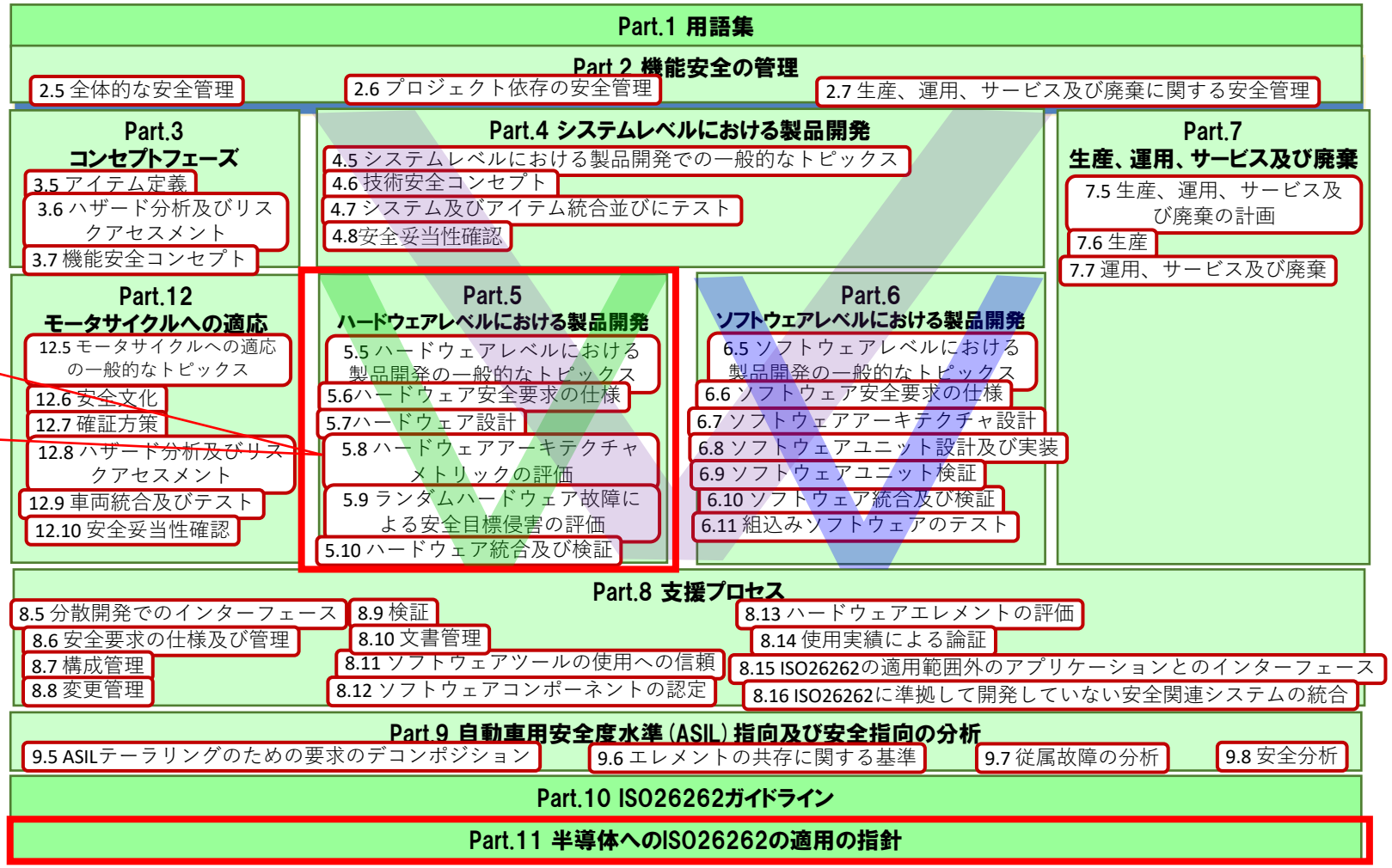
目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

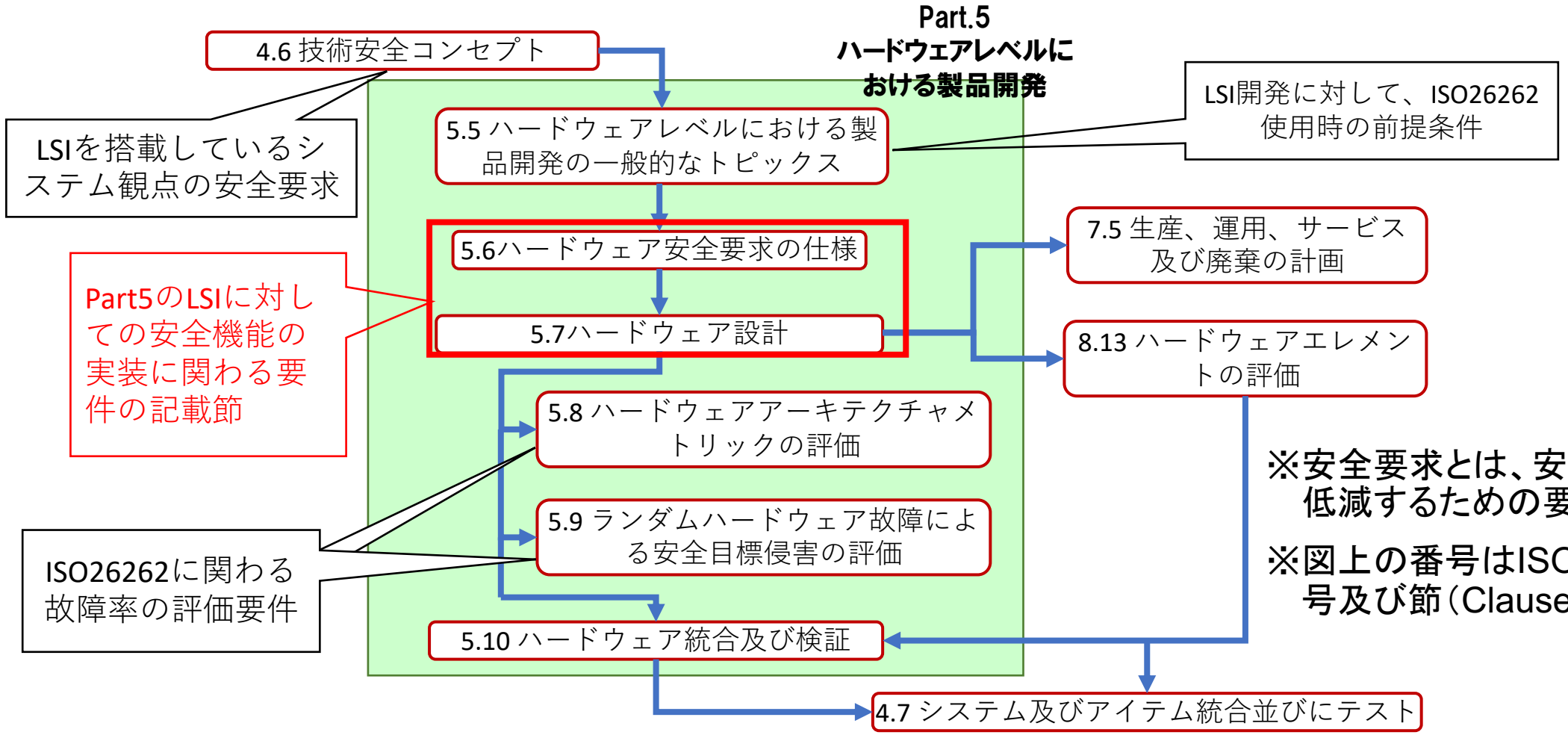
ISO26262規格(1/2):全体像

Part5：
「ハードウェアレベルにおける製品開発」

LSIに対しての安全機能の実装に関わる要件の記載章



ISO26262規格(2/2):ハードウェア開発フロー



※安全要求とは、安全な状態までリスクを低減するための要求

※図上の番号はISO26262の章(Part)番号及び節(Clause)番号

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

安全機構実装上の課題

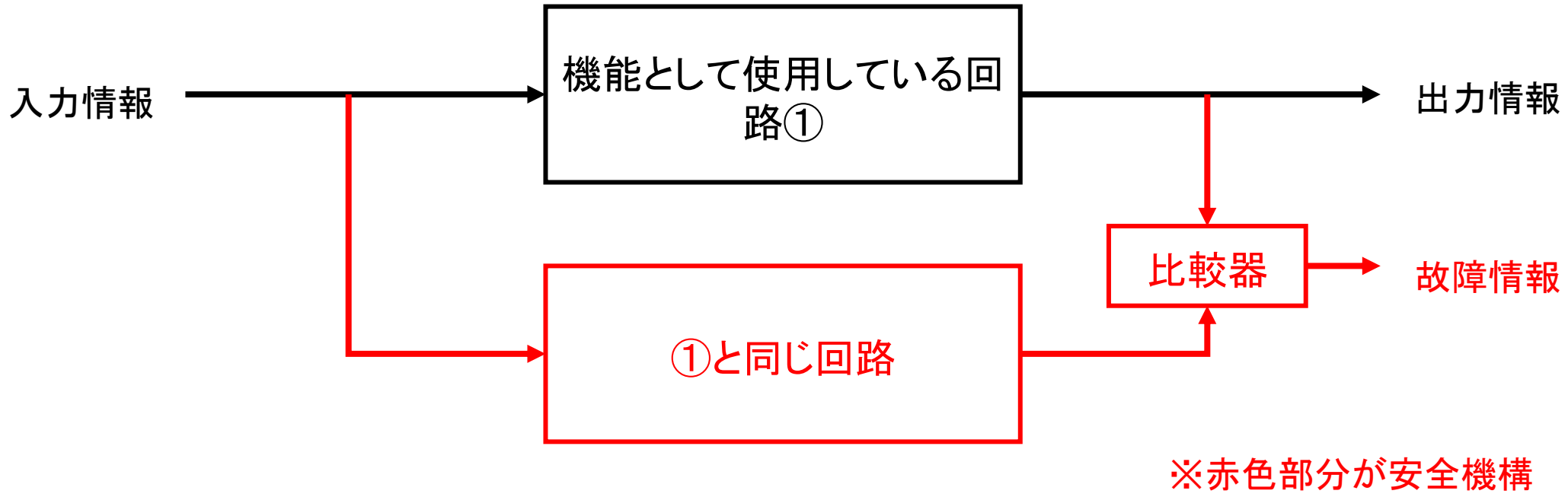
- 安全機構は、安全要求とLSI内部の個々のブロックの特性に応じたものを実装すれば良い。
- しかし、大規模LSIの場合、階層も深く、また実装されるブロック数も多い。このため、個々の内部回路の特性に応じた安全機構の検討することは困難である。よって、2重化（Dual lock step）タイプ等の、個々の特性を考慮しなくても良い安全機能が実装されるケースが多い。
- ２重化タイプは、回路規模は、必然的に2倍以上となり、消費電力の増大も招く。市場競争力のある機能安全対応LSIを開発するには、内部回路の特性に応じた安全機構の選択が重要である。

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

2重化(Dual lock step)タイプとは？

- 安全対策が必要な回路に対して、同じ回路を用いて入力情報に対して、出力結果を比較確認する安全機構です。設計済の同じ回路を使用し、比較確認するだけなので容易に設計できる。



目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

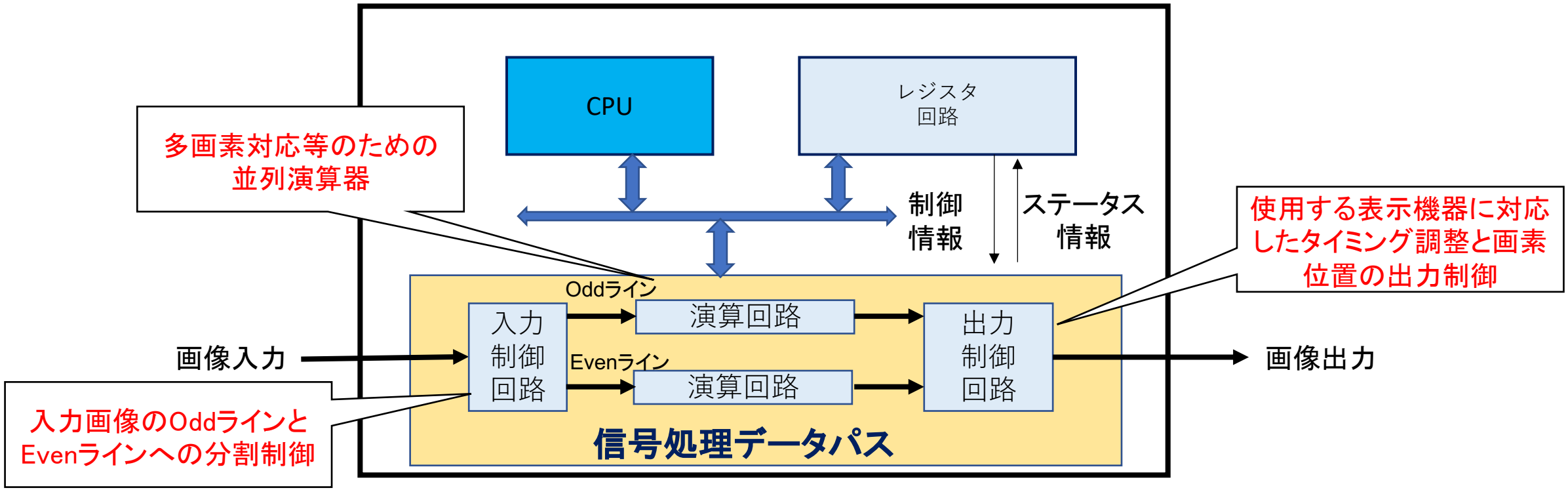
回路特性に応じた安全機構の事例紹介

次項以降に、ADAS（Advanced Driver-Assistance Systems, 先進運転支援システム）等で使用される画像系LSIを例に、回路特性に応じた安全機構の具体例を紹介し、回路規模・消費電力増を抑制できることを示す。

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

検討事例：典型的なリアルタイム画像処理LSI



リアルタイム画像処理は、上記のような構成となることが多い。

本事例に対する、回路増の小さい、安全機構の実装方法を紹介する

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

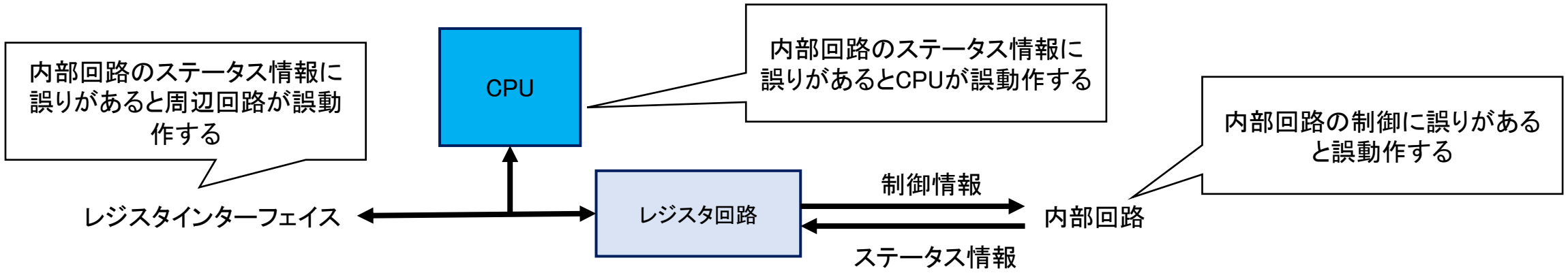
レジスタ回路事例(1/4):故障リスクと安全要求

レジスタ回路の故障リスク

- 誤制御入力による内部回路の誤動作
- ステータス情報の誤出力による周辺回路・CPUの誤動作

安全要求

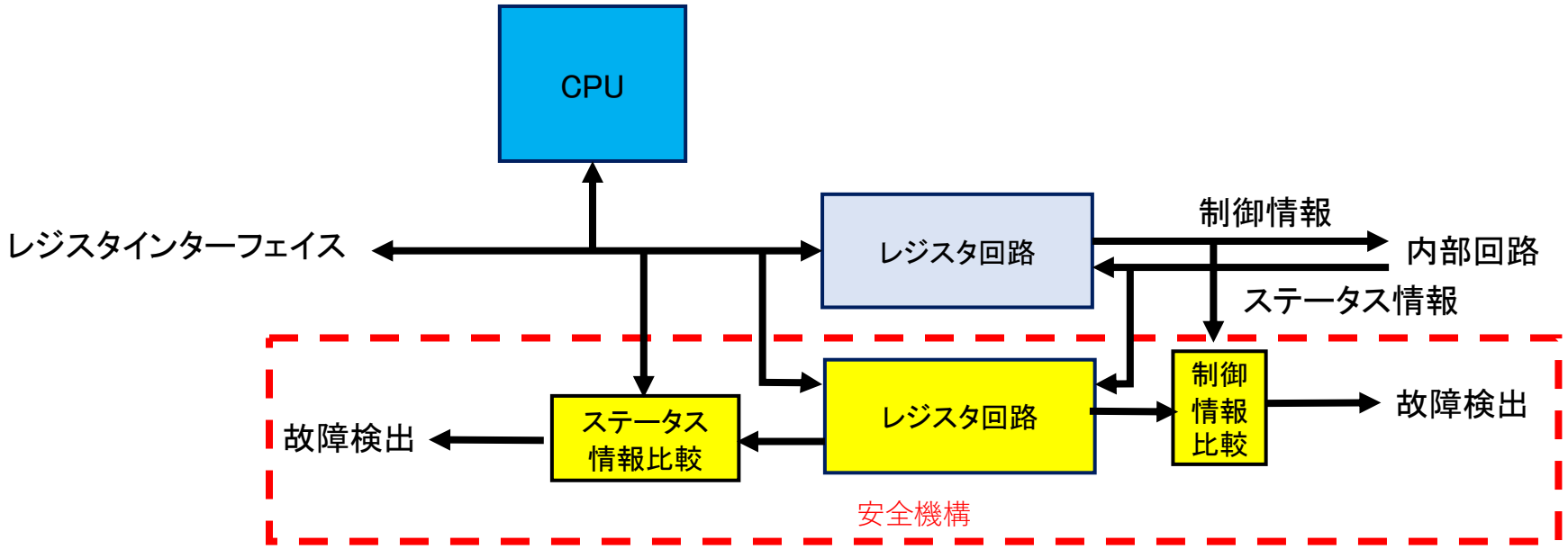
- レジスタ回路の制御情報の故障の検出と通知
- レジスタ回路のステータス情報の故障の検出と通知



レジスタ回路事例(2/4):2重化による安全機構

2重化タイプの安全機構

- レジスタ回路のアーキテクチャに依存しない



回路規模は2倍以上

レジスタ回路事例(3/4):CPUのSWによる安全機構

レジスタ回路の使用面での特長

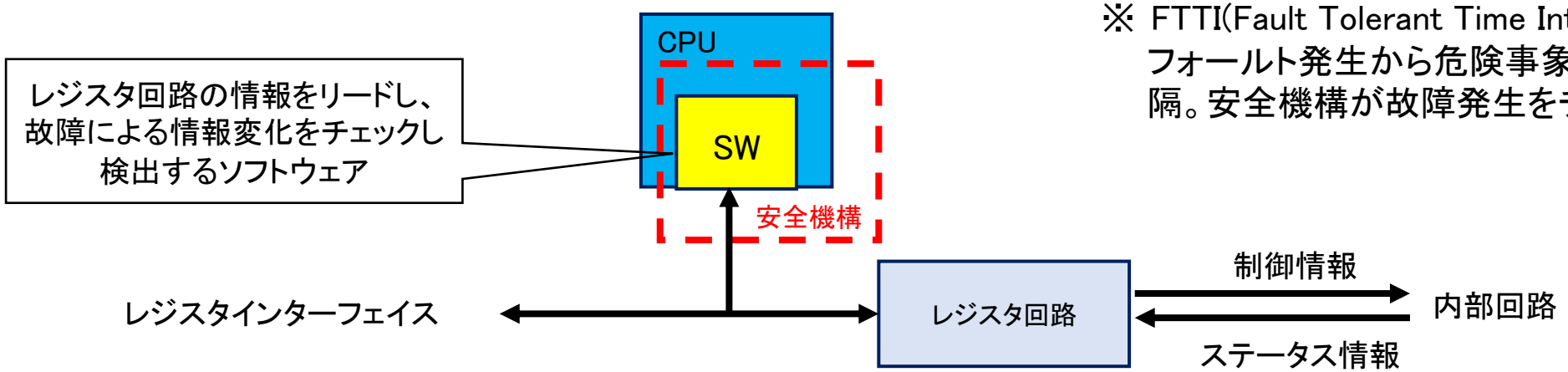
- レジスタ情報の更新間隔は、フレーム間隔より長い

本特長に考慮した安全機構

- 1フレームの期間内でレジスタ情報の故障の有無の確認が出来れば良い。
  ⇒ソフトウェアによるレジスタ値の確認でも、時間的に間に合う。

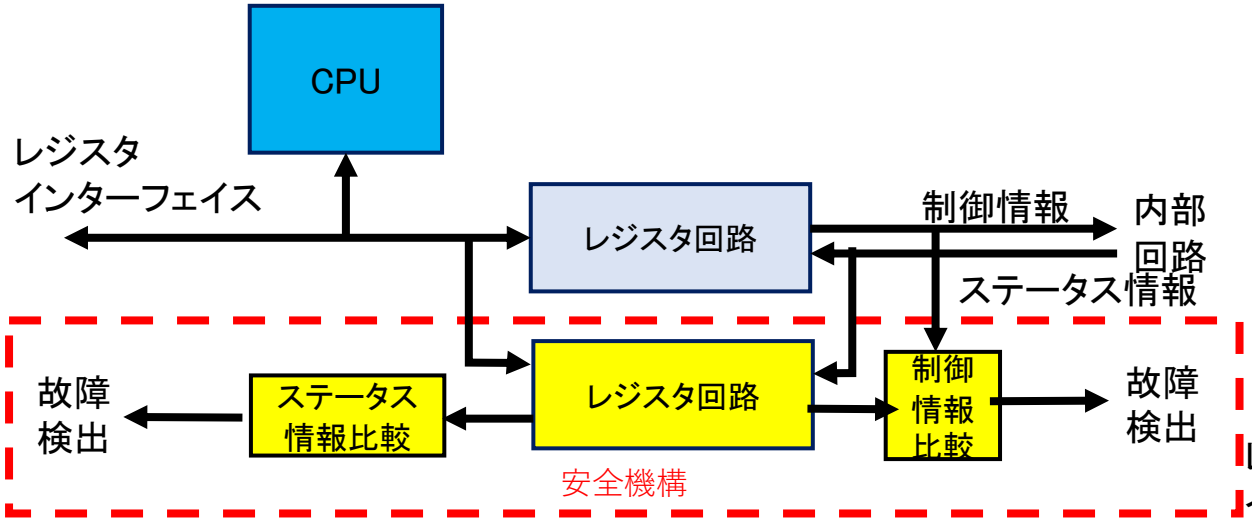
(FTTIが長いのでソフトウェアを使用した安全機構でも対応可能)

※ FTTI(Fault Tolerant Time Interval)
フォールト発生から危険事象発生までの間隔。安全機構が故障発生をチェックする時間。

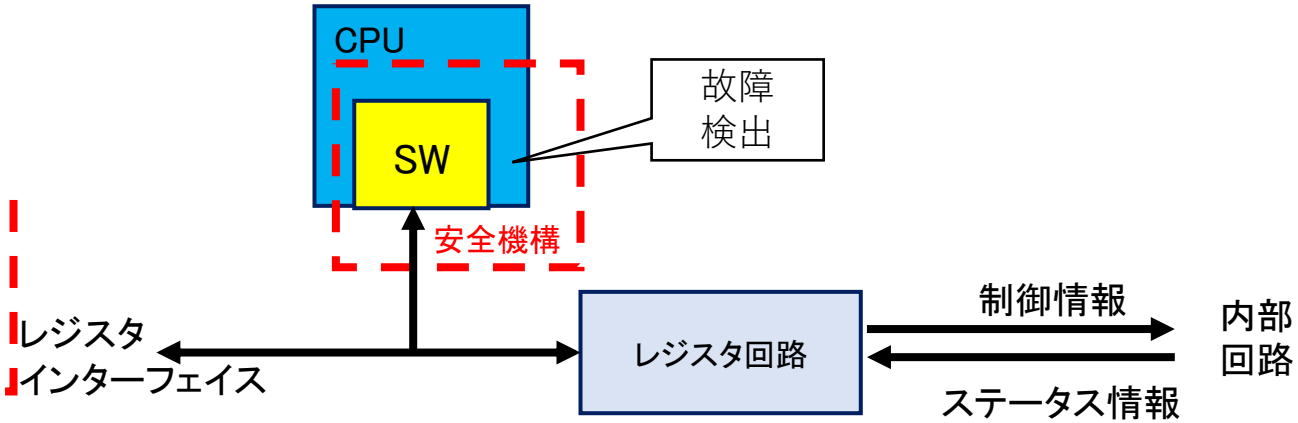


回路規模の増加無(SW処理が増加)

レジスタ回路事例(4/4):実装方法比較



2重化タイプの安全機構



回路特性を考慮した安全機構

2重化タイプは回路規模増が大きく、チップコストと消費電力面で不利

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

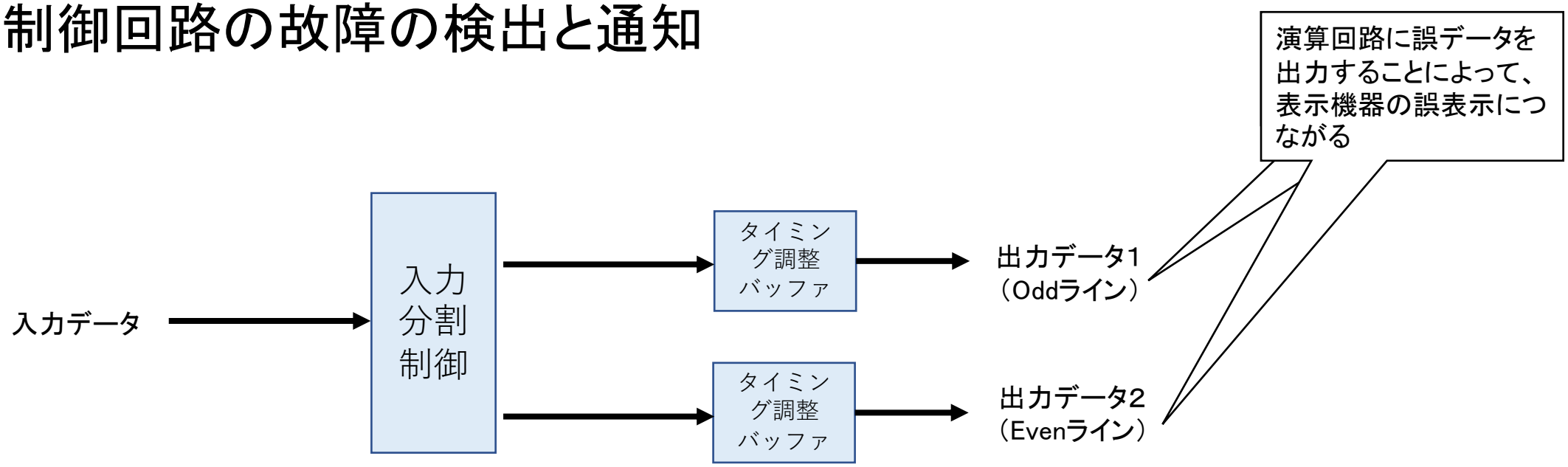
入力制御回路事例(1/4):故障リスクと安全要求

入力制御回路の故障リスク

- 故障による表示機器の誤表示

安全要求

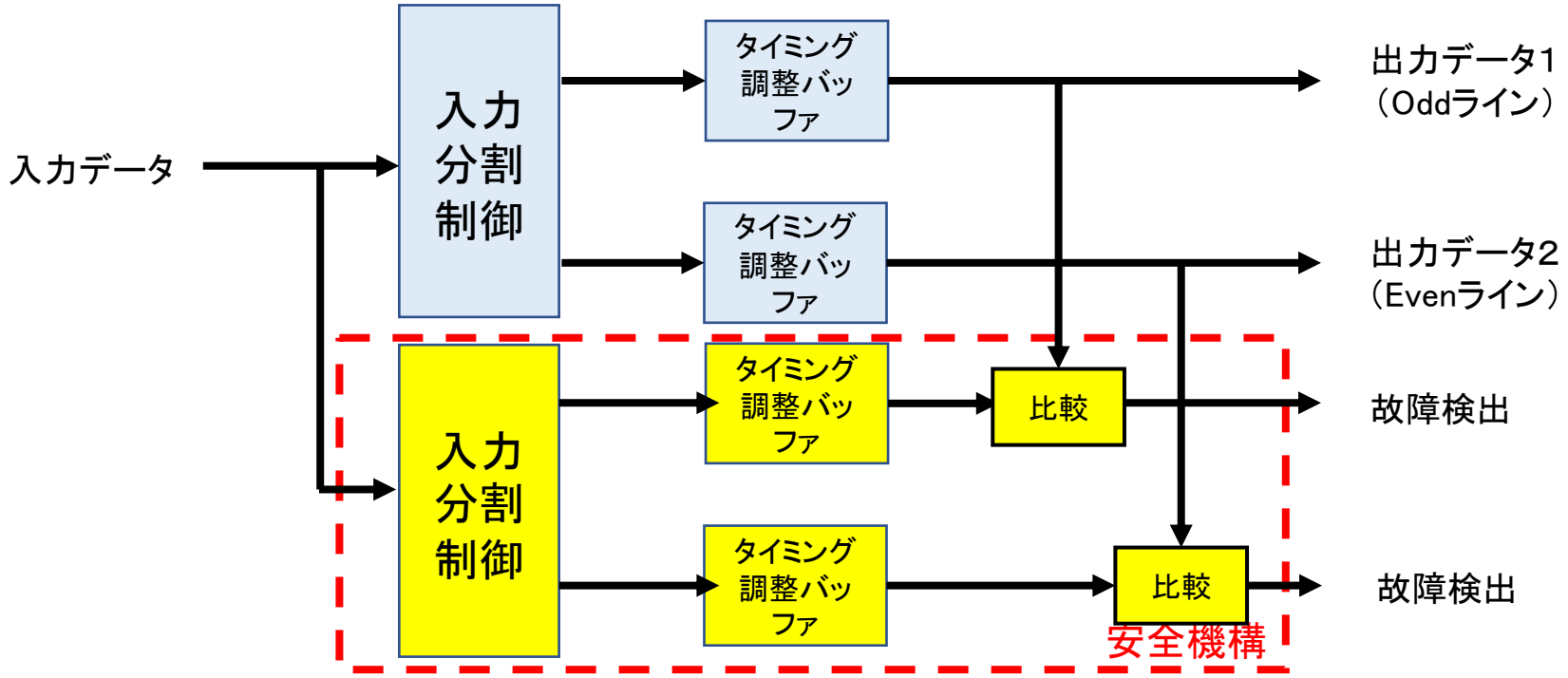
- 入力制御回路の故障の検出と通知



入力制御回路事例(2/4):2重化による安全機構

2重化タイプの安全機構

- 入力制御回路のアーキテクチャに依存しない



回路規模は2倍以上

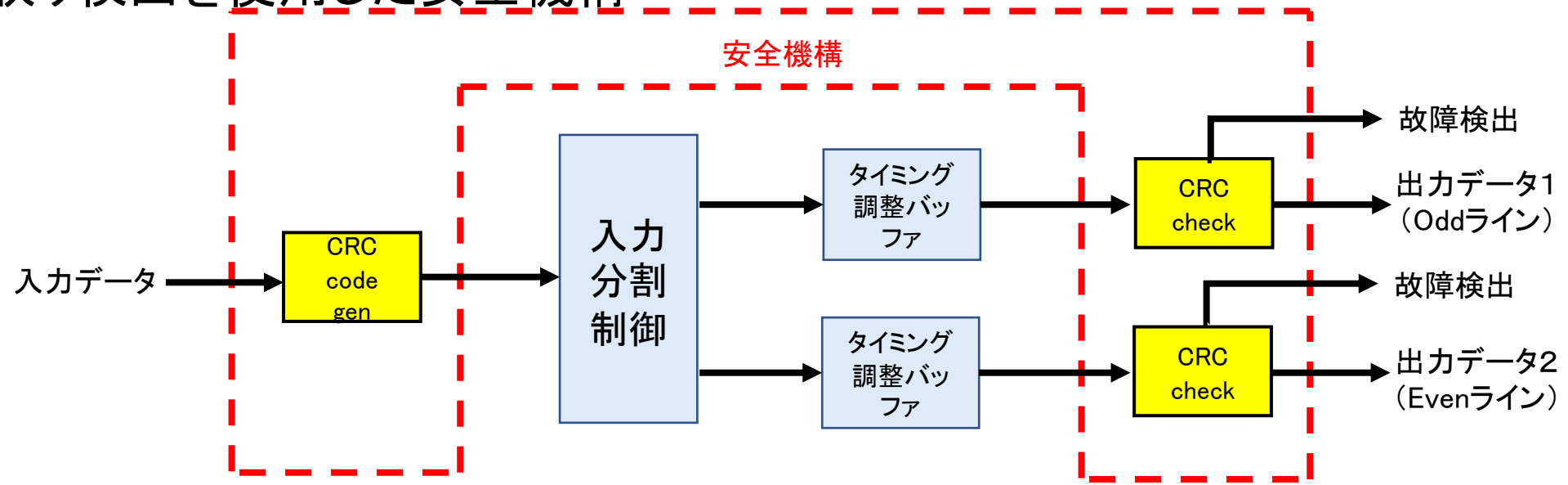
入力制御回路事例(3/4) : 誤り検出を使用した安全機構

入力制御回路のアーキテクチャの特長

- 入力制御回路内で画像データは変更しない。

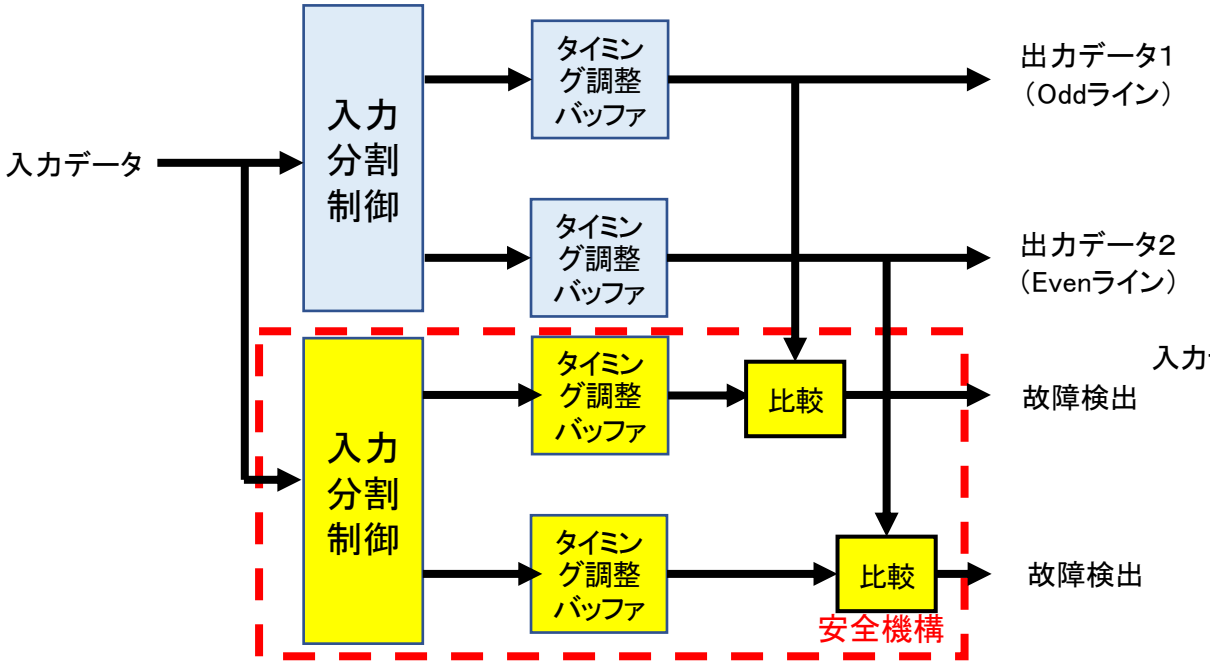
入力制御回路のアーキテクチャの特長に対応した安全機構

- 誤り検出を使用した安全機構

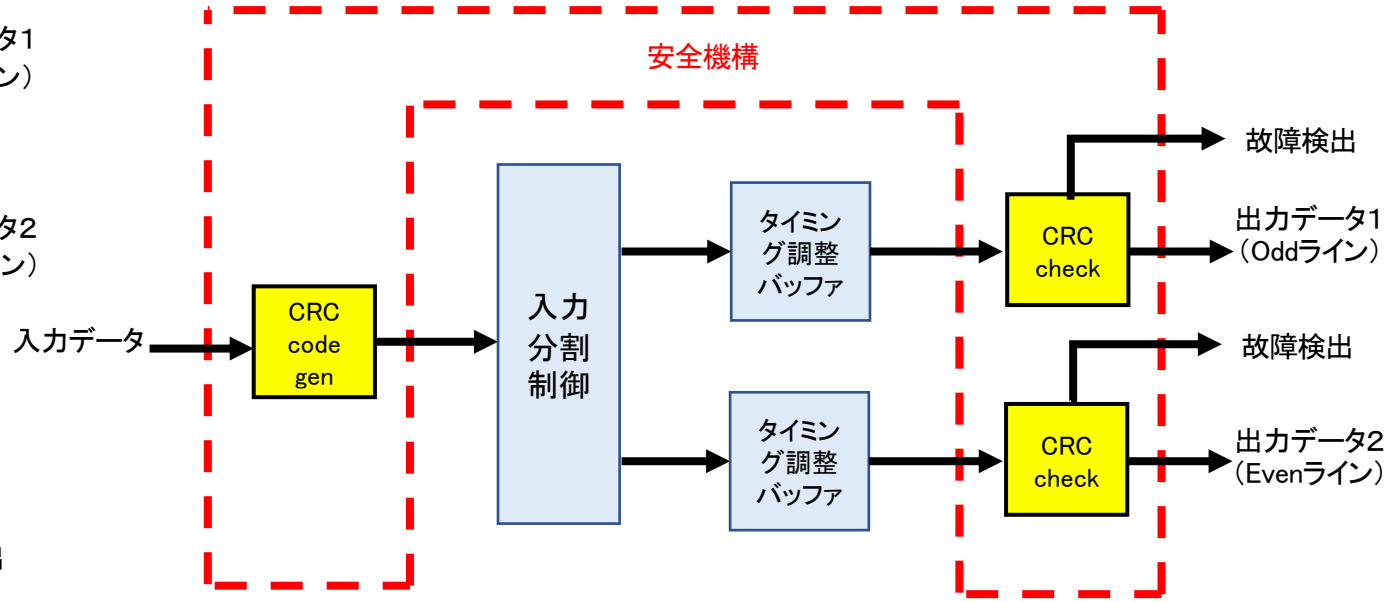


回路規模増は、CRC code genとCRC checkのみ

入力制御回路事例(4/4):実装方法比較



2重化タイプの安全機構



回路特性を考慮した安全機構

2重化タイプは回路規模増が大きく、チップコストと消費電力面で不利

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

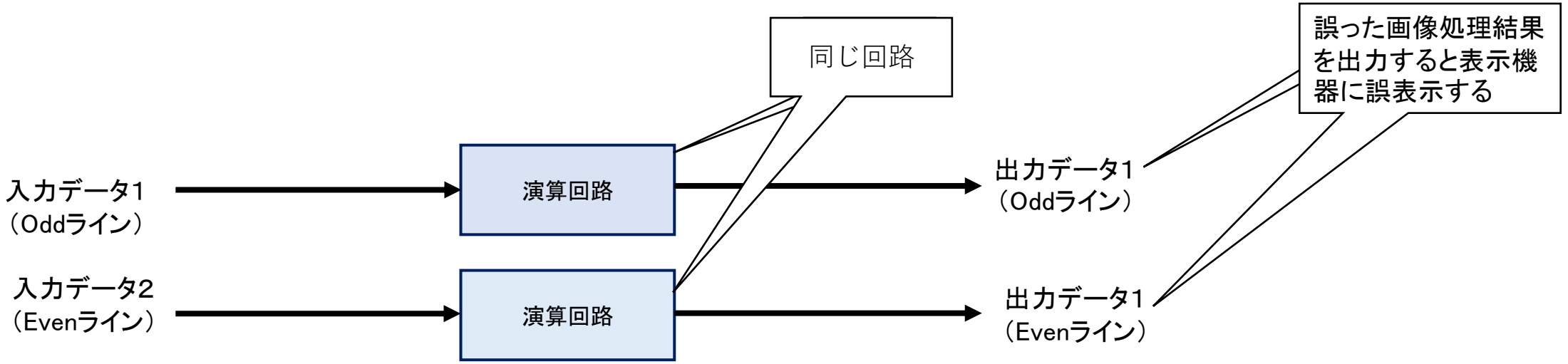
演算回路事例(1/4):故障リスクと安全要求

演算回路の故障リスク

- 表示機器の誤表示

安全要求

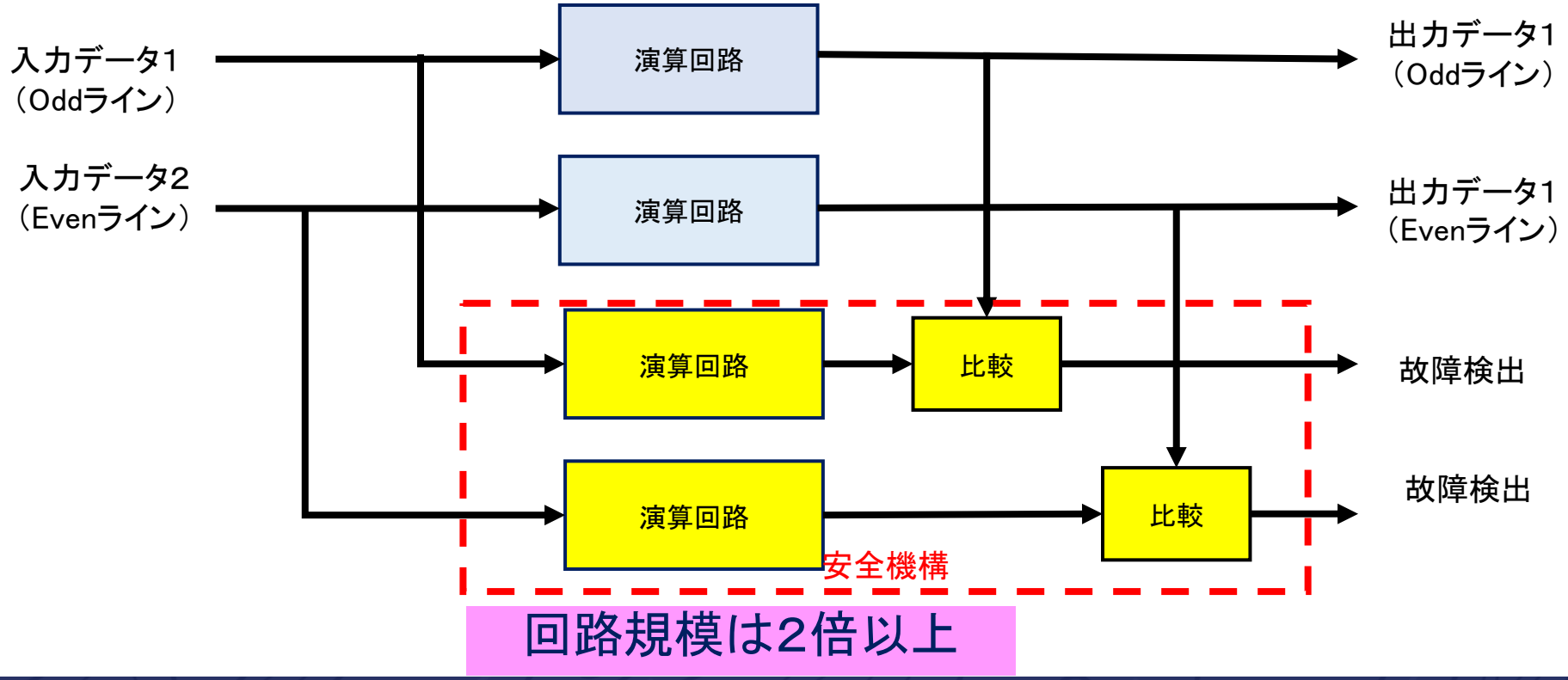
- 演算回路の故障の検出と通知



演算回路事例(2/4):2重化による安全機構

2重化タイプの安全機構

- 演算回路のアーキテクチャに依存しない



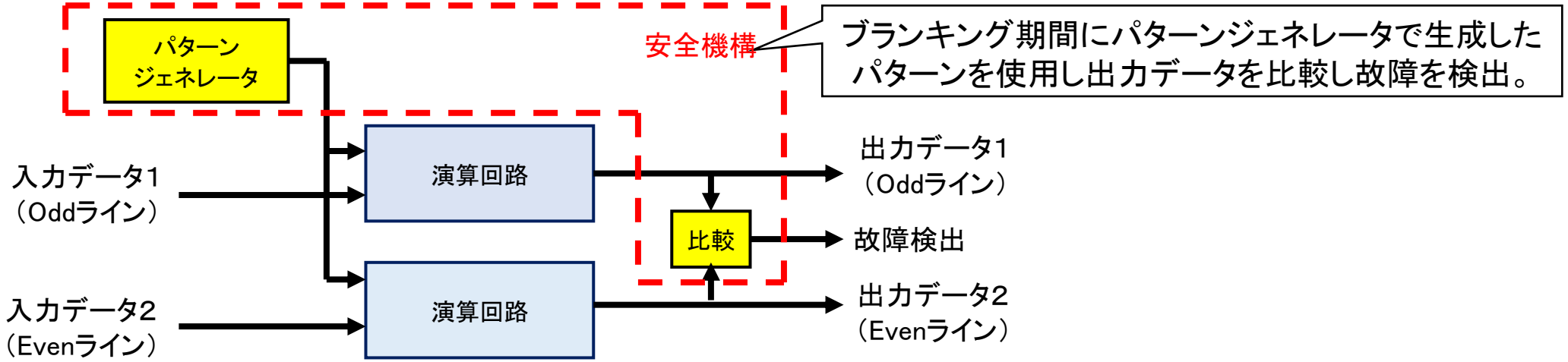
演算回路事例(3/4):並列演算器を活用した安全機構

演算回路のアーキテクチャの特長

- ブランキング期間に画像データ処理をしない期間がある
- 画像データ処理の高速化の為、同じ回路を並列で使用している。

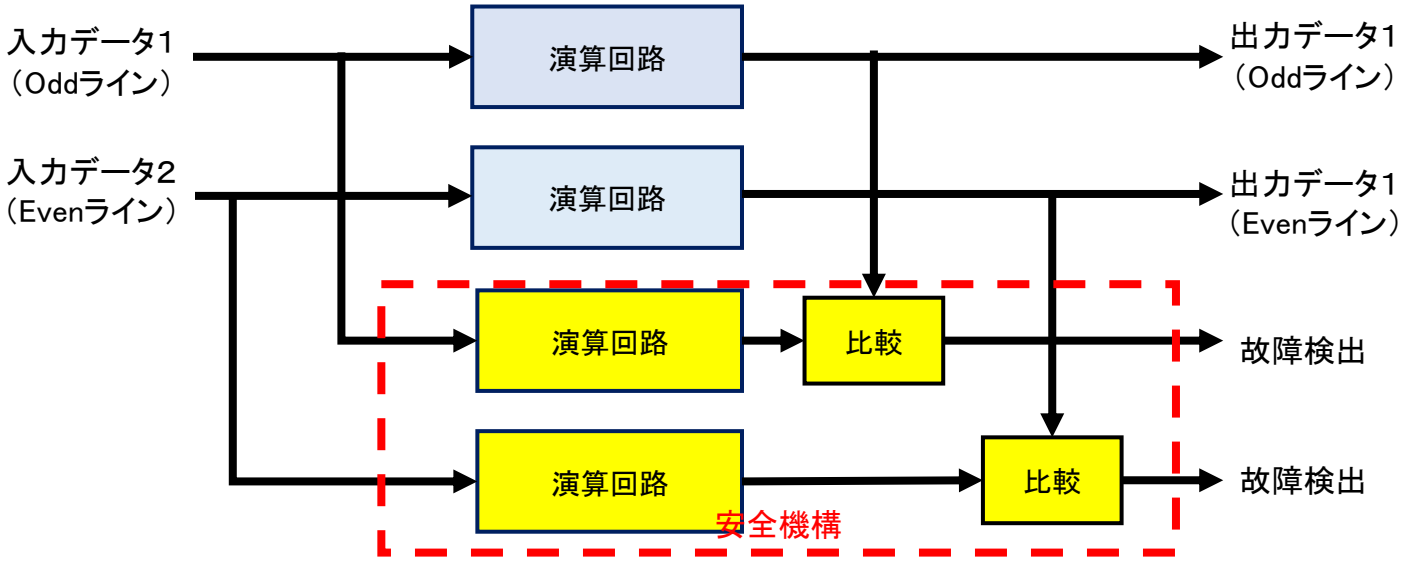
本特長を活用した安全機構

- ブランキング期間に通常動作で使用している回路を使用した安全機構

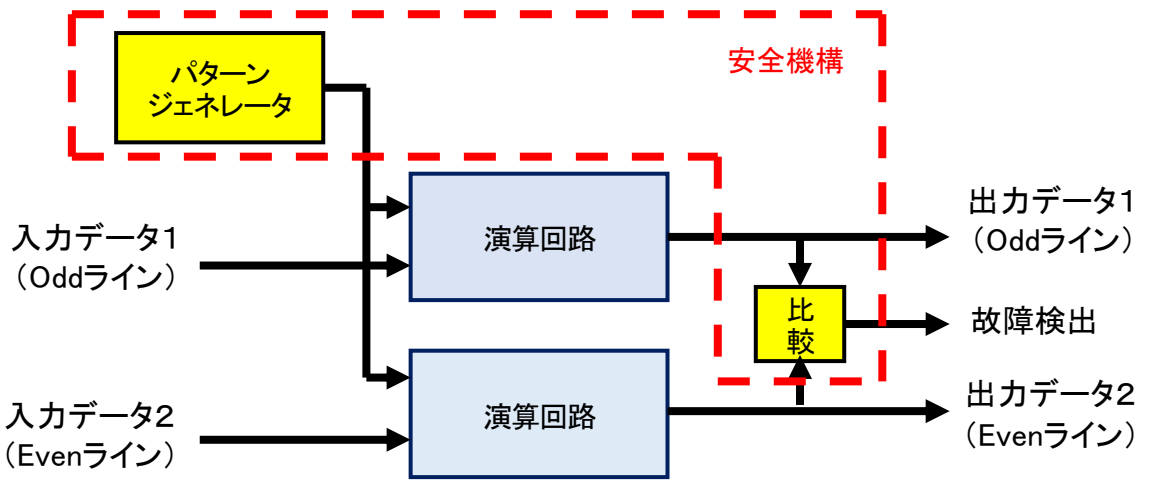


回路規模増は、パターンジェネレータと比較器のみ

演算回路事例(4/4):実装方法比較



2重化タイプの安全機構



回路特性を考慮した安全機構

2重化タイプは回路規模増が大きく、チップコストと消費電力面で不利

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

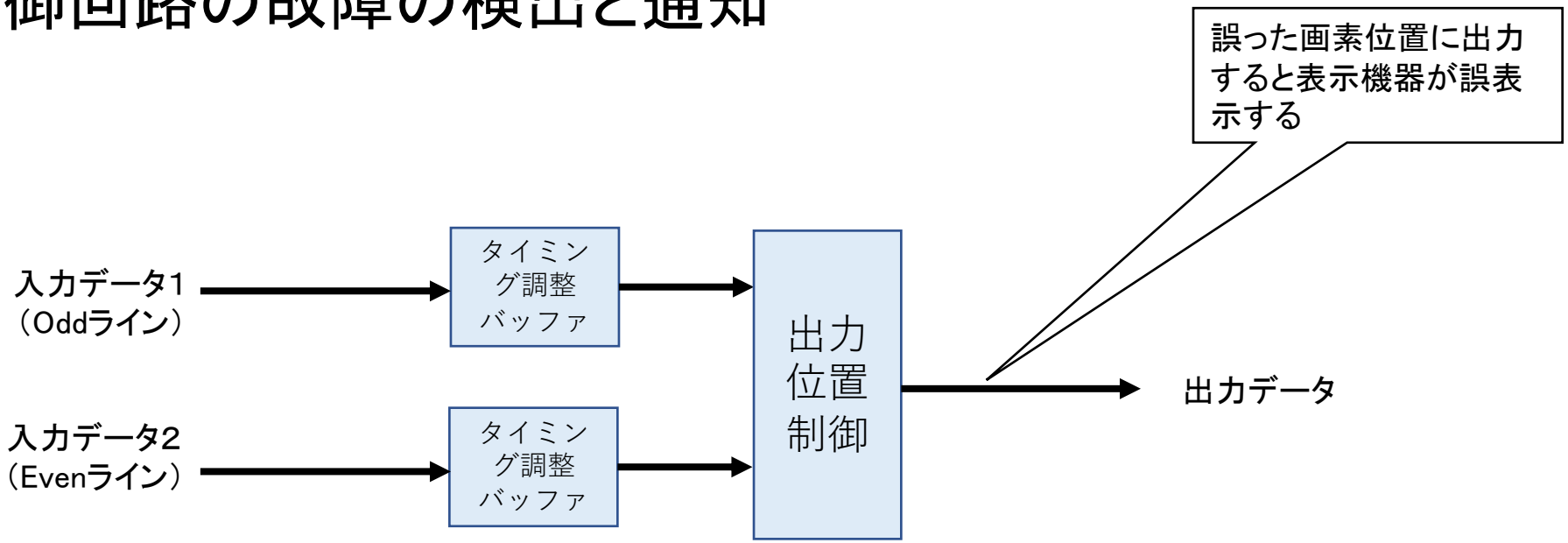
出力制御回路事例(1/4):故障リスクと安全要求

出力制御回路の故障リスク

- 表示機器の誤表示

安全要求

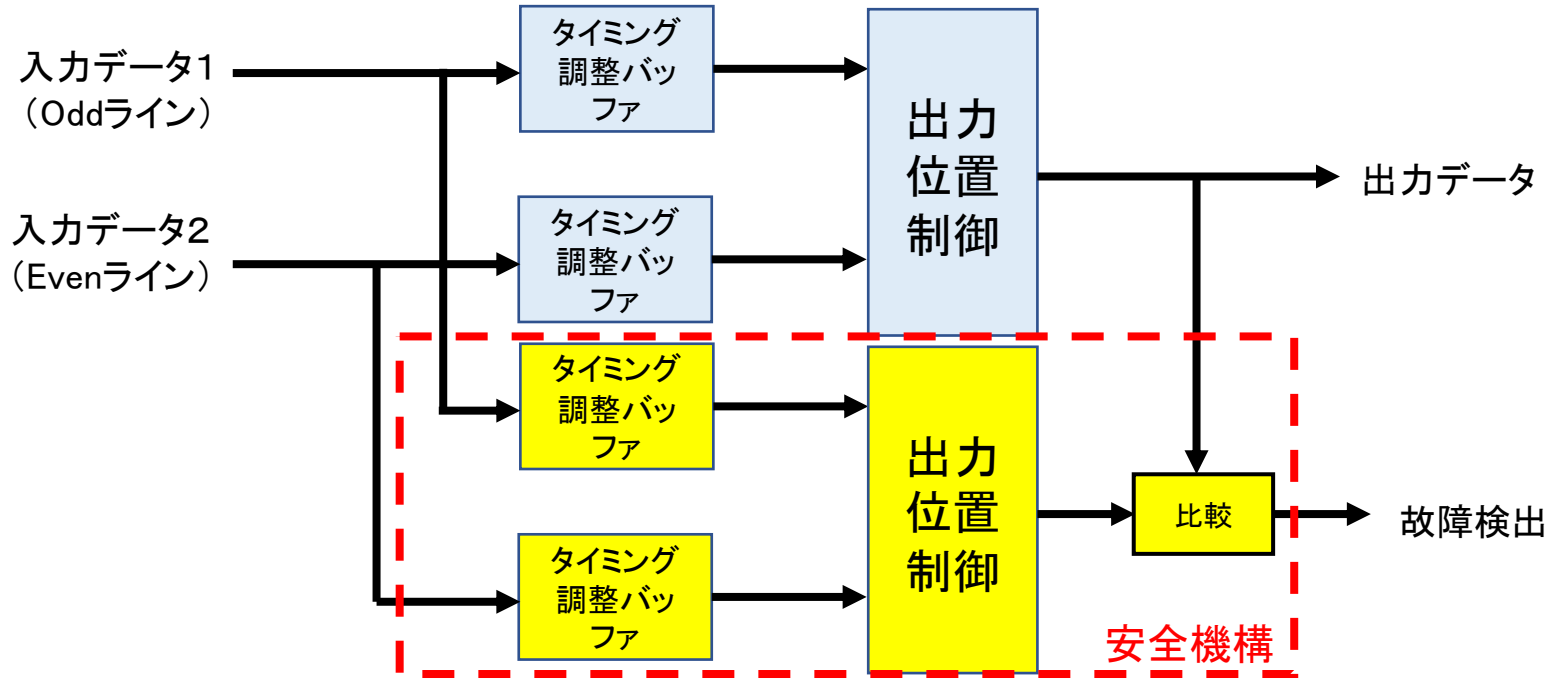
- 出力制御回路の故障の検出と通知



出力制御回路事例(2/4):2重化による安全機構

2重化タイプの安全機構

- 出力制御回路のアーキテクチャに依存しない



回路規模は2倍以上

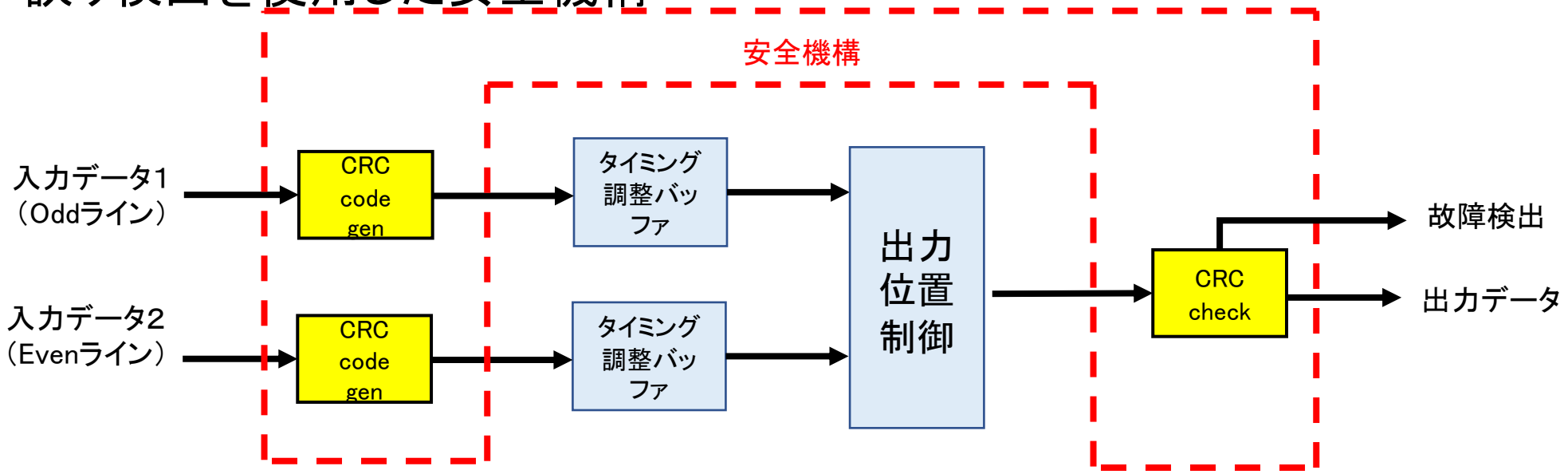
出力制御回路事例(3/4):誤り検出を使用した安全機構

出力制御回路のアーキテクチャの特長

- 出力制御回路内で画像データは変更しない。

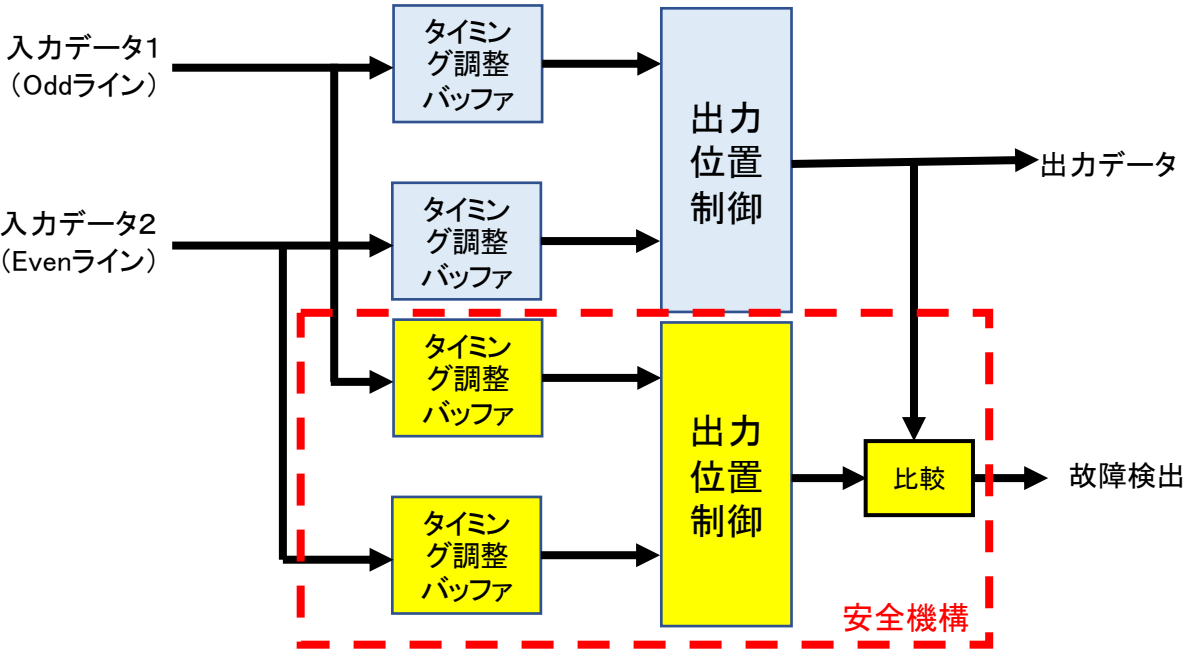
出力制御回路のアーキテクチャの特長に対応した安全機構

- 誤り検出を使用した安全機構

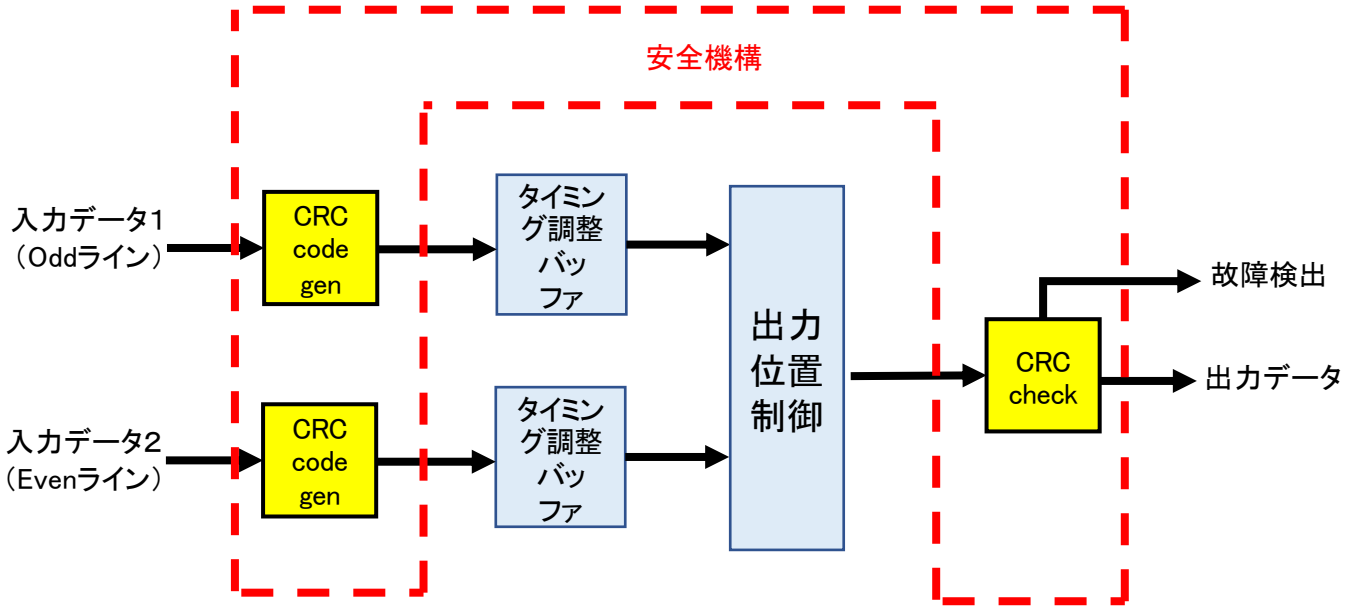


回路規模増は、CRC code genとCRC checkのみ

出力制御回路事例(4/4):実装方法比較



2重化タイプの安全機構



回路特性を考慮した安全機構

2重化タイプは回路規模増が大きく、チップコストと消費電力面で不利

目次

- 概要
- ISO26262規格の適用箇所
- 安全機構実装上の課題
- 2重化（Dual lock step）タイプとは？
- 機能安全アーキテクチャの検討事例紹介
  - 典型的なリアルタイム画像処理LSIの検討事例
  - レジスタ回路事例
  - 入力制御回路事例
  - 演算回路事例
  - 出力制御回路事例
- まとめ

まとめ

- 車載向けLSIには、ISO26262に準拠した設計が求められる。
- ISO26262に準拠する為には、安全要求に応じた安全機構の実装が必要となる。
- 単純な安全機構は2重化タイプであるが、回路規模や消費電力が2倍以上となる。
- 回路の用途や実際の利用形態を考慮することで、2重化タイプ以外の安全機構の実装が可能となり、回路規模/消費電力の増加が抑えられる。

質疑応答

最後までご聴講頂き、誠にありがとうございます。

ご質問があれば、ご質問お願いします。

後日、本プレゼンテーションについてご質問が発生した際は、下記までメールお願いします。

hamatani@vtech-inc.co.jp

ベリフィケーションテクノロジー株式会社　濵谷敏行