TI Live! TECH EXCHANGE

Japan Automotive Day

LVDS(FPD-LINK™)における機能安全設計

氏名　辻　慎治

概要 – このプレゼンテーションで取り扱う内容

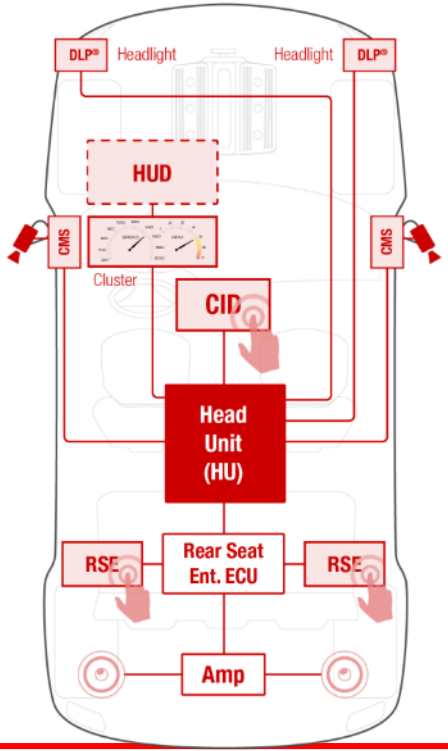
- このプレゼンテーションの内容
  - ASIL-B システムで FPD-Link™ を使用する例と検討事項
  - FPD-Link™ を使用するアプリケーション向けの SPFM と LFM の計算
  - FPD-Link™ 向けの各種診断モード
  - さまざまな指標を計算できるように FPD-Link™ チームが作成した関連資料
- このプレゼンテーションでは取り扱わない内容
  - ISO 26262 規格の包括的な概要
  - ISO 26262 と安全性の計算に関する包括的なトレーニング・コース

目次

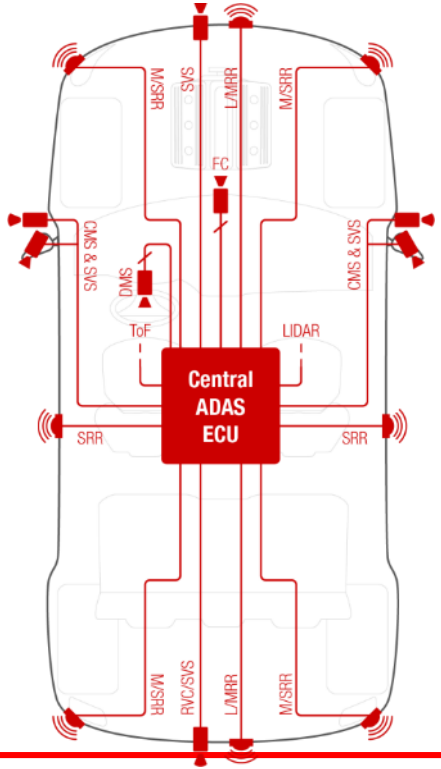
- 自動車のアーキテクチャ内での FPD-Link™ の使用事例
- さまざまな故障がシステム・レベルに及ぼす影響
- 一般的な車載クラスタディスプレイの安全性要件
- FPD-Link™ を使用する場合の機能安全に関する検討事項
- まとめ
- Q&A

TI の FPD-Link™

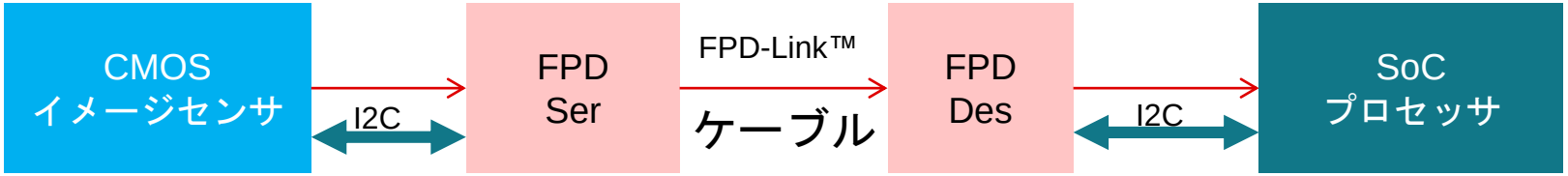
インフォテインメント用途の FPD-Link™



ADAS 用途の FPD-Link™

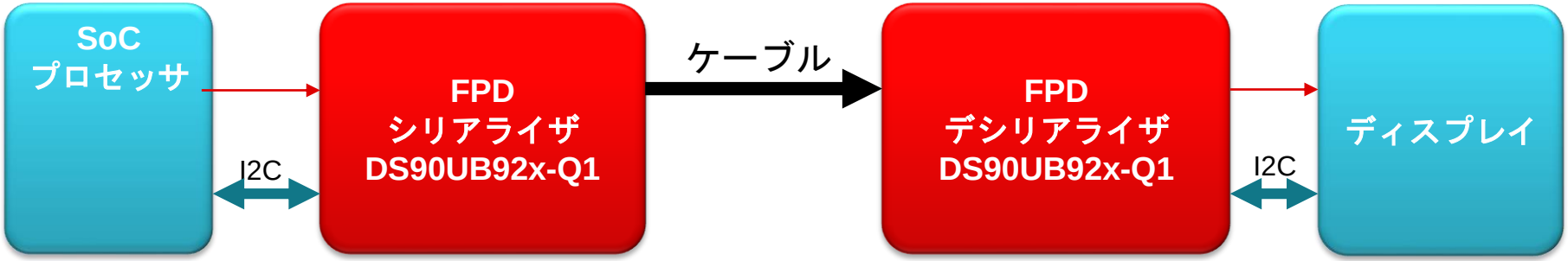


カメラを用いたビジョン・システムの例



- 上の図は 3 種類の高速インターフェイスを示しています
- 何かの部品の故障モードを含め、これらのインターフェイスのいずれかで問題が発生した場合、情報や画像の損失など、システム・レベルの影響が生じる可能性があります

クラスタ：インフォテインメント・システムの例



- SoC はビデオ / イメージのデータを FPD-Link™ 経由で送信します。
- いずれかのインターフェイスで、またはいずれかの部品内で問題が発生した場合、ピクセルの消失や、真っ暗で何も映らない暗転画面など、視覚的な影響を伴うシステム・レベルの問題が生じる可能性があります。

部品の故障がシステム・レベルに及ぼす影響

部品として使用している IC 内にある機能ブロックのいずれかで問題が発生すると、データ送信インターフェイスに影響を及ぼし、システム・レベルの故障モードにつながる可能性があります。ちらつき、表示の乱れ、不正確な表示、画像の固着、暗転などの画面になる可能性があります。

部品レベル

部品の故障

- レシーバ入力ブロック内の故障
- OLDI 出力ブロック内の故障
- クロック・ジェネレータ・ブロック内の故障
- クロック・データ・リカバリ・ブロック内の故障
- バック・チャネル・ブロック内の故障
- OLDI ドライバ・ブロック内の故障
- 電力ドメイン・ブロック内の故障
- I2C コントローラ・ブロック内の故障
- GPIO ブロック内の故障
- タイミングと制御ブロック内の故障
- モード選択ブロック内の故障

データ送信

データ送信

DSI / FPDLink™ / OLDI には、データ送信に関して類似する故障モードがあります。

- ビット・エラー
- リンク・ロス
- ……

システム・レベル

ディスプレイへの影響

- ディスプレイのちらつき
- 表示の乱れ
- 不正確な表示
- 画像の固着
- 暗転した画面
- インジケータの表示不可能

安全性要件の定義

安全性の目標

– ハザード分析やリスク評価の結果として導き出される、トップ・レベルの安全性要件

安全状態

– リスクを許容できる水準まで下げた、安全な動作状態

FTTI

– フォールト・トレラント時間間隔 (FTTI) とは、ハザードが発生せずにシステム内に故障が存在する時間です。

安全性要件の例：コックピットとクラスタディスプレイ

機能：

– コックピット SoC からディスプレイ・パネルまで、1 本のリンクを使用して表示データを送信

安全性の目標：

– ディスプレイ・パネルは正しいステータス・インジケータ (警告灯) を表示する必要があり、この安全性目標は ASIL-B レベルの要件として割り当てられます。

安全状態：

– 暗転した画面

FTTI：

– 500ms

ASIL の要件 | 偶発的故障のカバレッジ (範囲)

安全メカニズムの対象になっていない故障。安全性の目標に対する違反に直結。

	ASIL B	ASIL C	ASIL D
シングル・ポイント故障の指標 (SPFM)	90% 以上	97% 以上	99% 以上

マルチポイント故障。この種の故障が存在していても、単一の安全性メカニズムによる認識や検出が不可能。

	ASIL B	ASIL C	ASIL D
潜在的故障の指標 (LFM)	60% 以上	80% 以上	90% 以上

シングル・ポイント故障とマルチポイント故障に関する推定ハードウェア故障率。

ASIL	偶発的ハードウェア故障の確率的指標 (PMHF)	注
D	10^{-8} h^{-1} 未満 (10 FIT)	必須
C	10^{-7} h^{-1} 未満 (100 FIT)	必須
B	10^{-7} h^{-1} 未満 (100 FIT)	推奨

1 FIT = 10^{9} 時間ごとに 1 回の故障

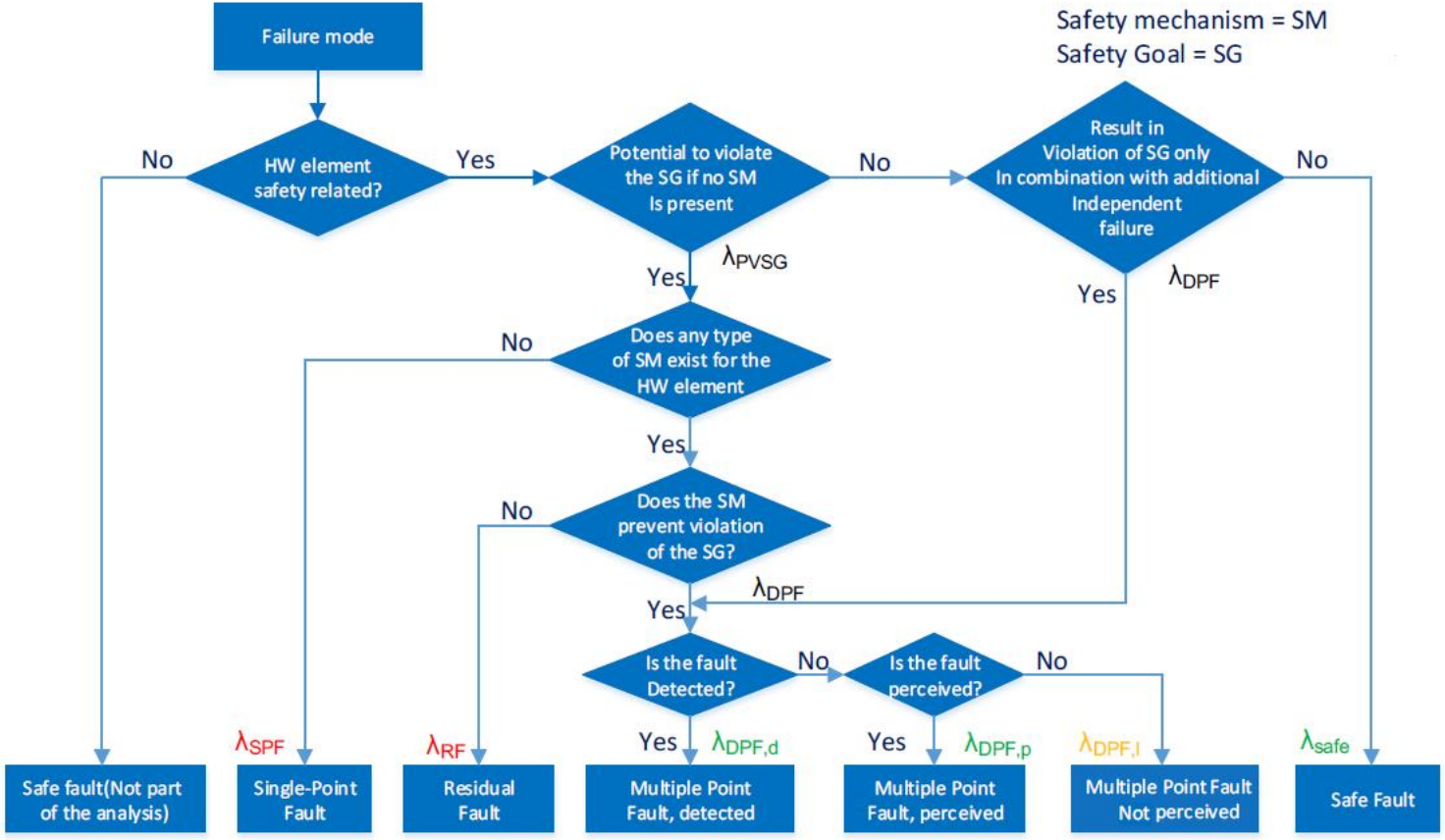
FMEDA とは

- Failure Mode Effects and Diagnostics Analysis (故障モード影響診断分析) の略称です。
- サブシステム / 部品レベルの故障率、故障モード、および診断能力を取得するための体系的分析手法です。
- この方式を使用して、SPFM 、 LFM 、 PMHFのアーキテクチャ指標を計算します。

FMEDA の一般的な計算手順

1. 安全性に関連するすべての要因を列挙
2. 各コンポーネントの FIT (時間あたりの故障回数) レートと FMD (故障モード分布) を列挙
3. 各コンポーネントの故障モードが及ぼす影響を判定
4. 各故障モードを分類
5. 各故障モードに対応する安全性メカニズムを定義
6. 各故障モードに対応する診断範囲を判定
7. SPM と LFM を計算

フローチャートの例 - 故障識別

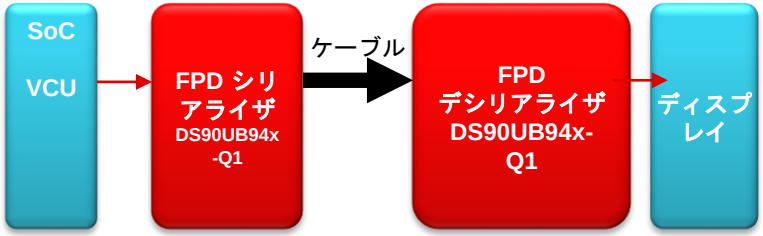


シングル・ポイント故障 – 例 1

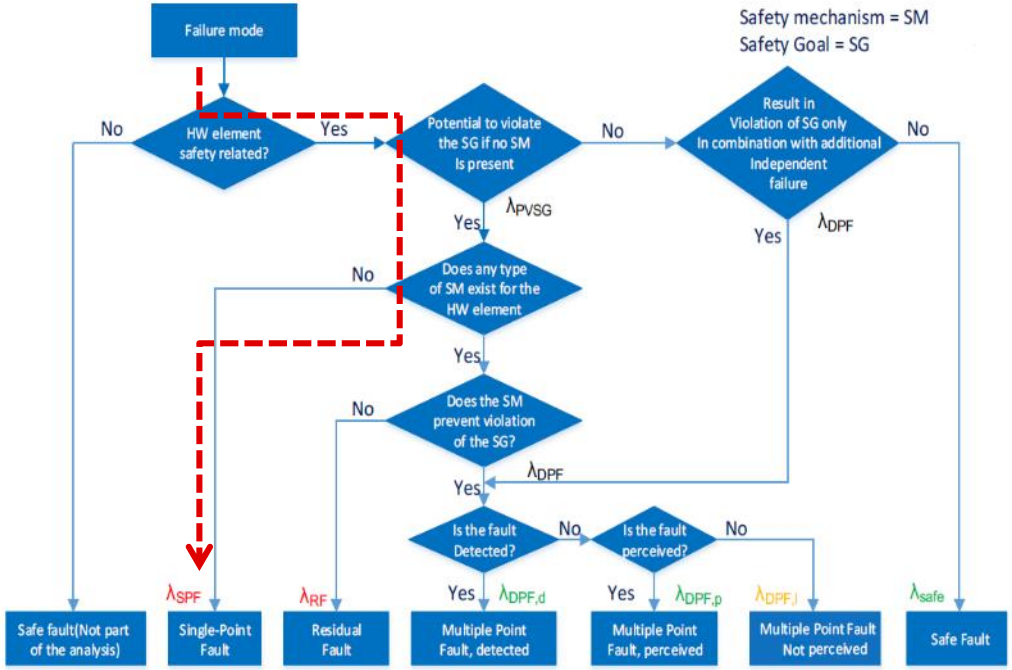
機能：シリアライザの高速データ出力をケーブルにシリアライザします

故障モード：出力電圧レベルが過度に小さく、Vid 仕様を下回っています

SM (安全機構)：この故障に対応する検出方式は存在しません。



この故障モードを分類する方法は？

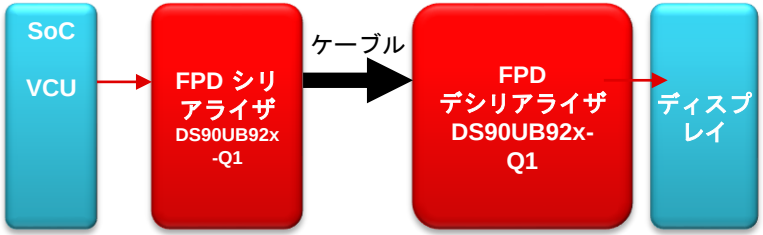


安全な故障 – 例 2

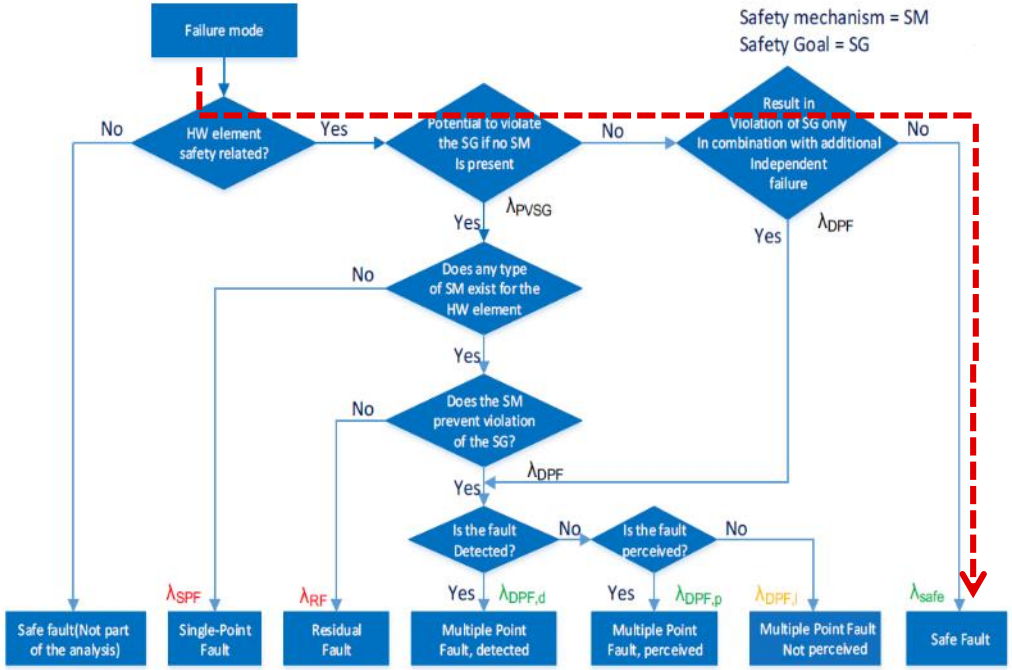
機能：シリアライザの高速データ出力をケーブルにシリアライザします

故障モード：出力電圧レベルがハイに固着

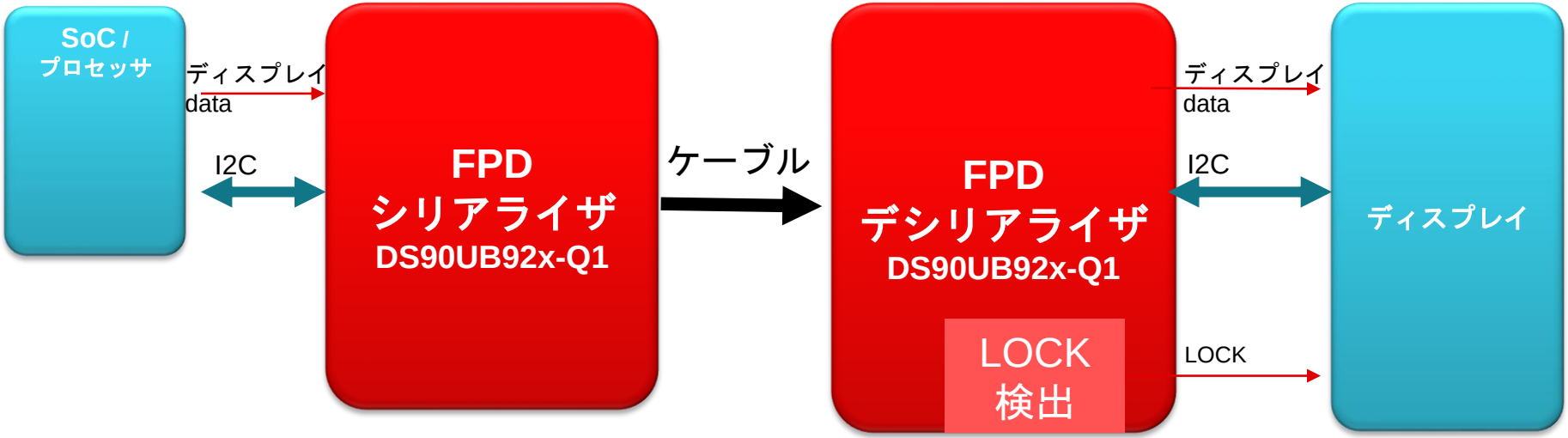
SG (安全性の目標)：安全性の目標に違反しません。この故障は画面の暗転という結果になるからです。



この故障モードを分類する方法は？



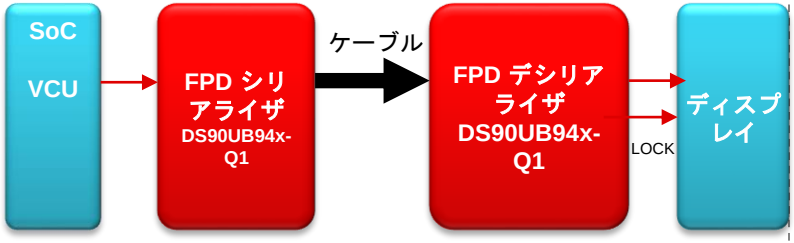
LOCK検出を安全性メカニズムとして活用



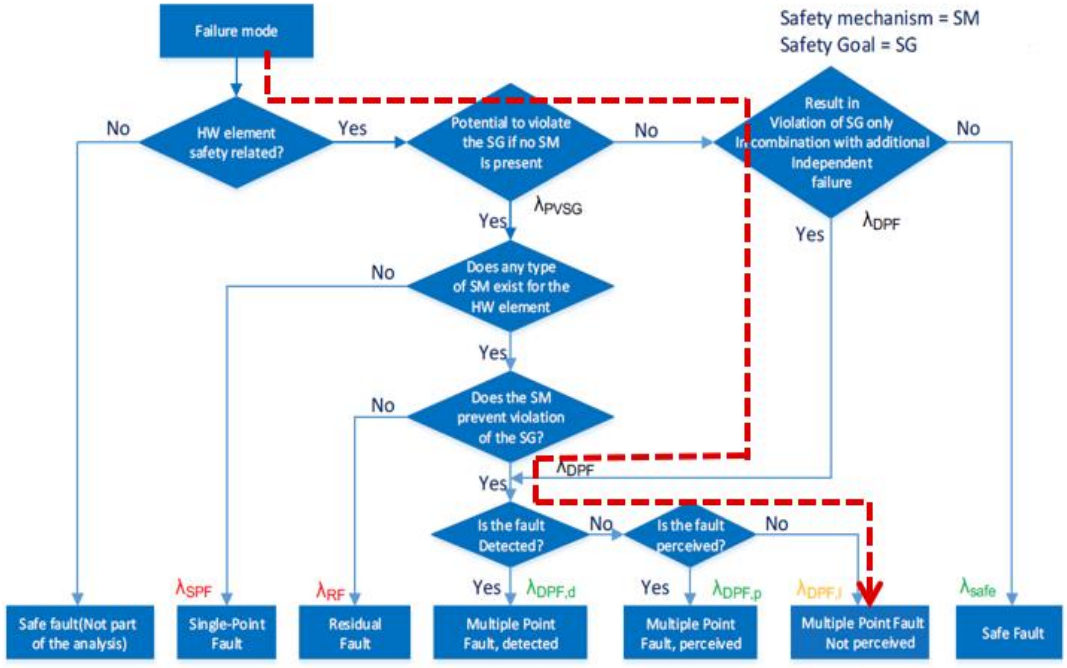
潜在的な故障 – 例 3

機能：ケーブルを通したシリアライザの高速データ伝送
故障モード：デシリアライザが出力した LOCK 信号がハイに固着

SM (安全機構)：LOCK 信号がハイに固着するという故障モードを検出する機構はないので、出力電圧が過度に低いという故障と組になった場合のみ、安全性の目標を侵害します。

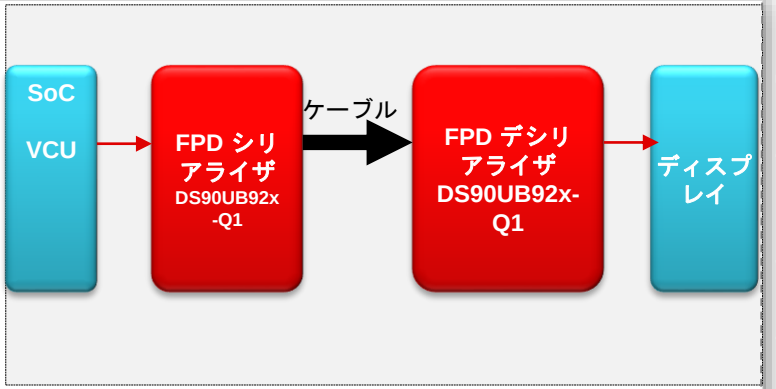


検出メカニズムを有しない“ロックがハイに固着する故障モード”は、潜在的故障として分類する必要があります。



LOCK 検出なし

LOCK 検出なしの場合の FPD-Link™



故障率のミッション・プロファイル：
シリアライザ (35 FIT) + デシリアライザ (35 FIT) = 70 FIT

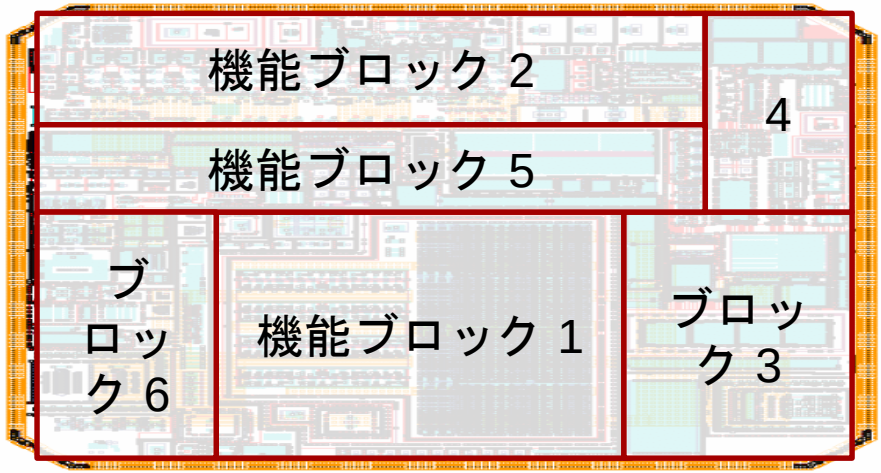
Failure Rate Mission Profile (1)	Per 10^9 Hours (FIT)
Total FIT Rate	35
Die FIT Rate	3
Package FIT Rate	32

LOCK を検出する場合は FIT が低減

故障モード	FIT	FMD %	LOCK 検出診断カバレッジ (範囲) (1-DC)	合計 FIT (安全機構なし)	合計 FIT (安全機構あり)
出力電圧がハイに固着	35	10%		0	0
出力電圧がローに固着	35	10%		0	0
出力電圧 Vod が過度に低い	35	70%	90%	24.5	2.45
出力電圧 Vod が過度に高い	35	5%		0	0
ピン間での短絡	35	5%		0	0
				24.5 FIT	2.45 FIT

FPD3 に関する故障モード分布 (FMD) の作成

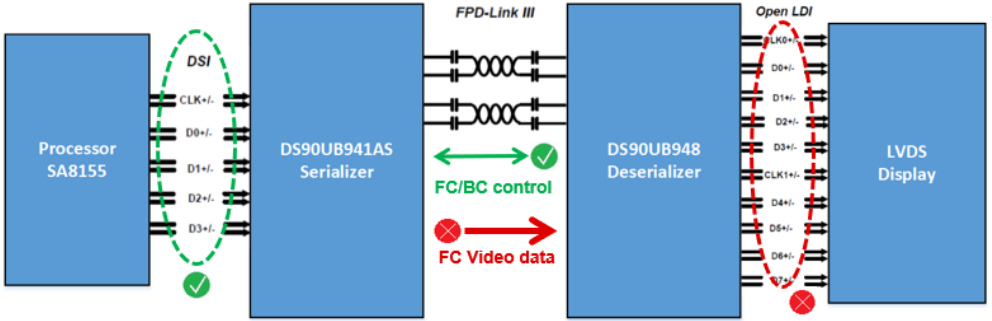
- FPD-Link™ に対応する FMD
  - FPD-Link™ の特定の IP ブロックに関連する障害モードは、シミュレーションに基づいて、または回路の知識 / 機能に基づいて計算されます



Example – FMEDA for an FPD-Link™ based system

Component	Function block	FIT rate	W FIT	Failure mode	Failure mode distribution	Does the failure mode violate safety goal	Safety mechanism	Diagnostic Coverage	Residual or single-point failure mode	Failure mode that may lead to the violation of safety goal in conjunction with failure of another block or component	Safety mechanism to prevent the failure mode being latent	Failure mode coverage with respect to Latent failure	Latent multi-point fault failure rate
Serializer	Driver	25		Output voltage stuck	25%	No							
		25	17.5	Output voltage Vod too low	70%	Yes	Yes	90%	1.05				
		25		Output voltage Vod too high	5%	No							
	PLL	10		Incorrect clock frequency	10%	Yes	No						
		10	12	Higher jitter	60%	Yes	Yes	90%	0.6				
		20		Clock stuck at a level	20%	No							
Deserializer	FPD data path	25	25	Incorrect data and clock recovery	100%	yes	yes	90%	2.5				
	oLDI data path	9	1.8	Incorrect output LVDS data	20%	yes	No						
	oLDI data path	9		LVDS output data stuck	70%	No							
	oLDI data path	9	0.9	LVDS output clock timing mismatch	10%	Yes	No		0.81				
	LOCK	1		LOCK stuck high	25%	No				Yes	No	0%	0.25
		1		LOCK stuck low	25%	No							
		1	0.5	Incorrect LOCK decode	50%	Yes	No		0.5				
			57.7						5.46				0.25
	SPFM		0.905										
	LFM		0.995										

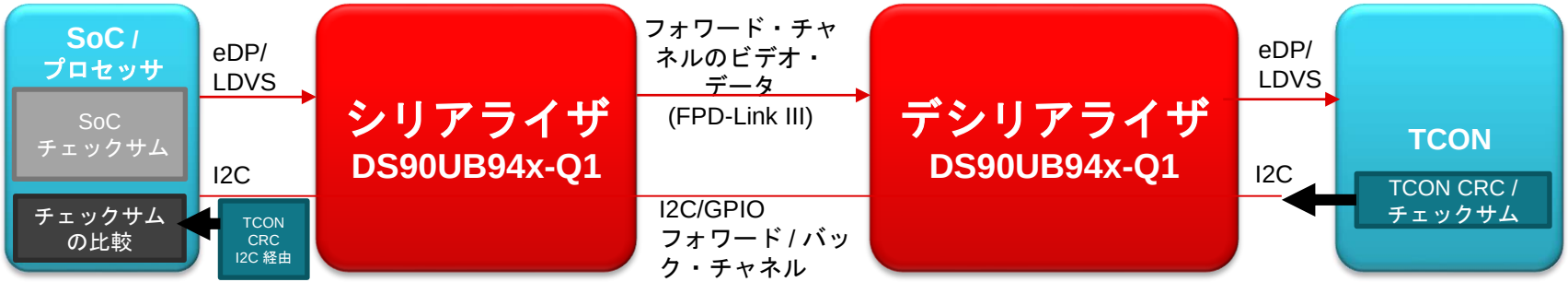
FPD-LinkIII で利用できる各種診断機能



機能	故障モード	検出方式	DC
DSI	• ビット・エラー • リンク・ロス	• 16 ビット CRC、シングル・ビット / マルチビット ECC • DSI/DPHY エラーを検出するための DPHY_DLANEx_ERR レジスタ • DSI プロトコル・エラーを検出するための DSI_STATUS レジスタ • DSI エラーを報告するためのメイン・レジスタの GENERAL_STS (0x0C)	高
FC/BC 制御データ	• ビット・エラー • 通信の喪失	• CRC チェック • BCC ウォッチドッグ・タイマ	高
FC ビデオ・データ	• ビット・エラー • リンク・ロス	• UB948 内の LINK_ERROR_COUNT (0x41) • UB941AS 内の GENERAL_STS (0x0C) • ディスプレイのタイミングに関するエラー状態を提示するための LOCK/ PASS ピン	中
Open LDI	• ビット・エラー • リンク・ロス	• CRC / ECC / Parityいずれのチェックもなし • DES を使用してこれらのエラーを検出することはできないので、ディスプレイ側に頼る必要があります。	“Low”

FuSa：プロセッサ内での CRC の比較

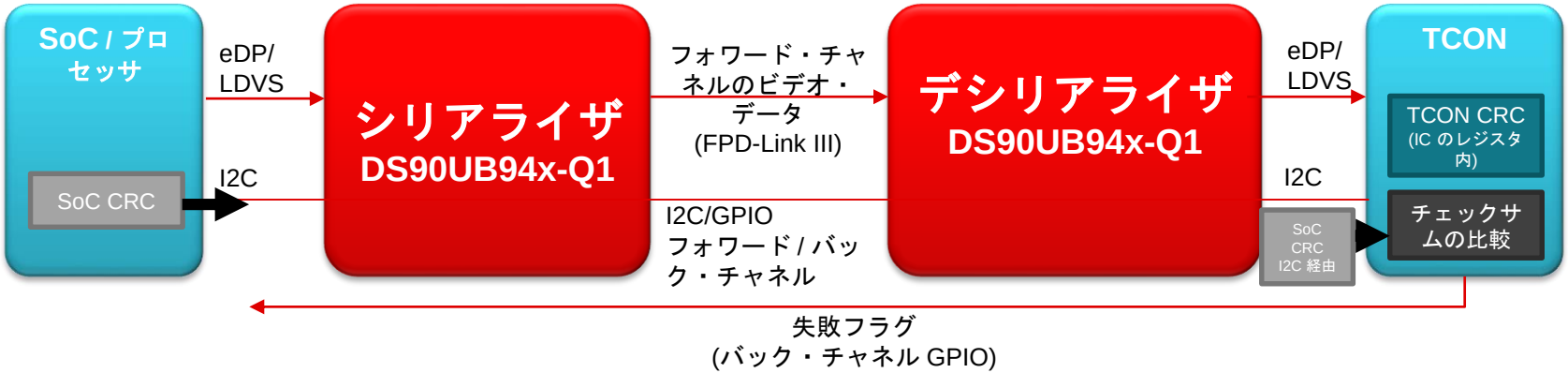
- TCON は CRC を計算し、バック・チャネル I2C を経由してコックピット SoC に送り返します。
- SoC は CRC を計算し、TCON の CRC 結果と比較します。



CRC とチェックサムの計算や比較を行うために、追加の SoC ソフトウェアが必要です。

FuSa：TCON 内での CRC の比較

- SoC は CRC を計算し、フォワード・チャネル I2C を経由して TCON に送り返します。
- TCON は CRC を計算し、TCON の CRC 結果と比較します。



CRC とチェックサムの計算や比較を行うために、追加の SoC ソフトウェアが必要です。

FuSa：監視

- 一般的に、セーフティ・インジケータのみが ASIL-A/Fusa を必要とします。
- 機能安全に対応する一部のマイコンは、これらのインジケータのピクセルやフレームに関するチェックサムを事前にプログラムしておくことができます。
- 特定の状態に関して、マイコンは自動車のCANバスまたはフォワード・チャネルからインジケータのステータスを取得することができます。

まとめ

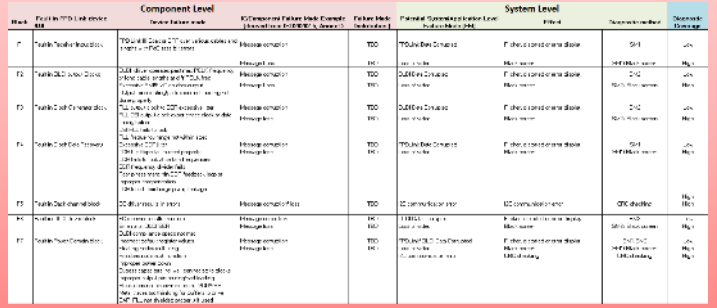
まとめ – ASIL-B クラスタ・システムで FPD-Link™ を使用する場合の検討事項

- 安全性の目標とは
  - 画像全体または複数のインジケータのみ
- 安全状態とは
- FPD-Link™ のバージョンは？
  - FPD-Link III、FPD-Link IV
- タイミング・コントローラ (TCON) は？
  - TCON の内蔵機能は？ (CRC、CRC の比較と生成、OSD)
- ディスプレイ・モジュール内のマイコンの有無は？ マイコンが存在する場合、どのような機能や能力があるか？ (処理能力、通信機能など) 型番は？
- どのインフォテインメント・プロセッサ (SoC) を使用しているか？ 型番は？

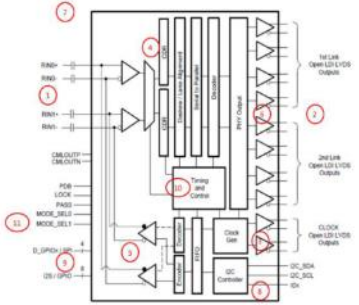
TI の関連資料

- 顧客の安全性の目標、安全状態
- SER/DES、TCON、マイコン、SoC、電源などを含めたシステム・ブロック図
- 顧客の診断能力、CRC、OSD は？

- デバイスの故障モードをシステム・レベルの故障モードにマッピング
- システム・レベルから診断カバレッジ（範囲）を改善



TI が提供するデータ：デバイスの FIT レート、故障モードと分布、システムへの影響



Total die area 7075600

Total FIT rate 35

Function	Function Area	Function Distribution	Failure Mode	Failure Distribution Partial of Function	Failure Distribution of Device	Failure description and effect	Failure Rate (FIT)
FPD_Driver	33,060	0.47%	Output Saturated High	35%	0.16%	Output of the driver will be stuck to high. Link will be lost.	0.057
			Output Saturated Low	35%	0.16%	Output of the driver will be stuck to low. Link will be lost.	0.057
			Incorrect output impedance	10%	0.05%	Unstable link or no link	0.016
			VOD Too High	10%	0.05%	Link will be achieved but may have potential EMC issues	0.016
			VOD Too Low	10%	0.05%	Unstable link or no link	0.016
CLOCKGEN (FPD_PLL)	710,942	10.05%	PLL CLK Frequency Incorrect	30%	3.01%	Output rate incorrect. Bandwidth may be limited or link lost.	1.055
			PLL unstable - does not settle	40%	4.02%	Link will be lost.	1.407
			PLL Clock phase offset	20%	2.01%	Link will be lost.	0.703
			PLL Clock Saturated High	5%	0.50%	Link will be lost.	0.176
			PLL Clock Saturated Low	5%	0.50%	Link will be lost.	0.176
FPD_Serializer	4,415	0.06%	Serializer Data Bit(s) Saturated High	45%	0.03%	FPD output data stuck high. Link will be lost.	0.010
			Serializer Data Bit(s) Saturated Low	45%	0.03%	FPD output data stuck low Link will be lost.	0.010
			Frame clock off or at wrong frequency	10%	0.01%	Unstable or no lock.	0.002
BC_Receiver	176,398	2.49%	Output Saturated High	20%	0.50%	BC_receiver output stuck high. Lost of back channel	0.175
			Output Saturated Low	20%	0.50%	BC_receiver output stuck low. Lost of back channel	0.175
			Improper gain or bandwidth settings	30%	0.75%	Unstable back channel communication. Error could occur or lost	0.262
			Incorrect VID	30%	0.75%	Unstable back channel communication. Error could occur or lost	0.262

TI 製品の機能安全クラスと提供される資料

		Functional Safety-Capable	Functional Safety Quality-Managed*	Functional Safety-Compliant*
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA**	✓	included in FMEDA	included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)**			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate***			✓