自己修復機能を有する3次元VLSIシステムの創製　小柳G

デンソー 情報安全事業グループ 鎌田

国際機能安全規格(IEC61508)

電気・電子回路及びマイコンを用いた安全性確保の規定　2000年　①設計ミス

自動車業界ではISO26262(IEC61508ベース)が調達要件になってきた

故障

1.決定論的原因故障　→全安全ライフサイクルの考えを導入

2.ランダムハードウェア故障

ISO26262でもASIL(Automotive Safety Integrity Level)　②故障率

つまり受容出来るリスクを達成するために必要なリスク低減レベルが規定されている

暴露確率(E0-E4)　遭遇する頻度

制御可能性(C0-C3)　回避行動の難易度　→　ASIL(A,B,C,D)/QM

危害度(S0-S3)　危害の大きさ　危険側故障目標値:FIT

レーンンキープアシストシステム(LKA)の一例 :E4,C2,S3→C(100FIT以下)

また障害検出能力(SPFM,LFM)に関する規定が存在する　③故障検出

ただしアルゴリズムの不完全さによる誤認識による誤動作などに関しては用例などの記述は無く何らかの考察が必要と考える　④誤認識

@ DENSO confidential / DENSO corporation reserves all rights, including rights of disposal such as copying and passing on to third parties.

ASIL(Automotive Safety Integrity Level)の判定方法

E:暴露確率

Class	E0	E1	E2	E3	E4
内容	信じ難い	極めて 低い確率	低い確率	中程度の 確率	高い確率

C:制御可能性

Class	C0	C1	C2	C3
内容	全体的に 制御可能	簡単に 制御可能	普通に 制御可能	・制御が難しい ・制御不可能

S:危害度

Class	S0	S1	S2	S3
内容	障害 無し	・軽傷 ・中程度 の障害	重い、 生命関わる障害 (生存の見込みはある)	・生命を脅かす障害 (生存の見込みは不確実) ・致命傷

判定表

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

QM:要求無し(通常の品質管理で良い)の意味

ISO26262-5 Annex Gで目標FIT値

Level	目標FIT値
D	<10FIT
C	<100FIT
B	
A	<1000FIT

障害検出能力(SPFM,LFM)

SPFM: Single Point Faults Metric
→危険に至る全障害の中で単一障害以外の割合

LFM: Latent Faults Metric
→危険に至る多重障害の中で組み合わせ障害以外の割合

ISO26262-5 Annex Eで目標値

Level	目標SPFM	目標LFM
D	>99%	>90%
C	>97%	>80%
B	>90%	>60%
A	-	-

システムに対する要求値ASIL(FIT),SPFM,LFMをどう部品に割りつけるのか？

@ DENSO confidential / DENSO corporation reserves all rights, including rights of disposal such as copying and passing on to third parties.

危険側故障率と部品の故障率の関係
危険側故障率＝故障率*(1-自己診断率/100)　・・・ ISO26262-5 Annex C
故障率＝Σ(素子故障率*危険側故障モードの発生割合の和)　・・・ 同 Annex F
素子故障率：汎用故障率DBとしてIEC62380,IEC61709など

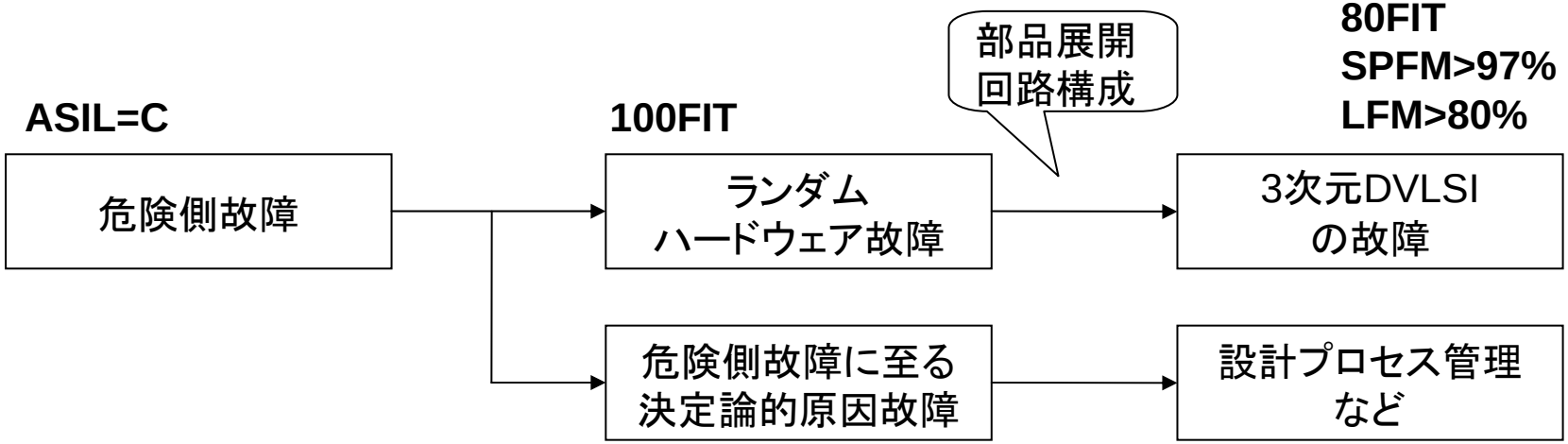
システム(危険側)故障率の部品への割り振り
センサ35% + 電子回路15% + アクチュエータ50%　が「通例*」
*電子回路に対してはやや厳しい見積もり
電子回路内
受動部品　・・・ IEC62061 Annex D
能動部品　・・・ IEC62061 Annex D 未規定時は均等割り が「通例」

ASIL=Cの例で
危険側故障率<100FITが要求
自己診断率97%(=システム要求と同じと仮定)とすると 故障率=3,300FIT
内電子回路には15%となる500FITを割り当て
危険側故障モードの発生割合の和を50%とすると 素子故障率=1,000FIT
受動部品が1FIT*200個 能動部品が当該DVLSI合わせて10個あるとすると
当該DVLSI素子故障率=(1,000-1*200)/10=80FIT
ex1: @ASIL=B,C 自己診断率97% 素子故障率80FIT
ex2: @ASIL=D 自己診断率99% 素子故障率10FIT

システム構成の仮定に基づけば部品に展開することが出来る

@ DENSO confidential / DENSO corporation reserves all rights, including rights of disposal such as copying and passing on to third parties.

自動車の運転支援システムは色々な商品が考えられるしシステム構成も個別だが
ASIL=Cを例として以下を目標として検討する
（最終的にはASIL Dの製品もあり得るので視野には入れる）



3次元DVLSIのデペンダビリティ目標値
・故障率<80FIT ・SPFM>97% ・LFM>80%

今後 ①ディペンダビリィティの目標値を達成する方式の評価方法の検討を行う
②誤認識の問題を再考察する

@ DENSO confidential / DENSO corporation reserves all rights, including rights of disposal such as copying and passing on to third parties.