車載アプリケーション向け
マルチチップネットワークオンチップ

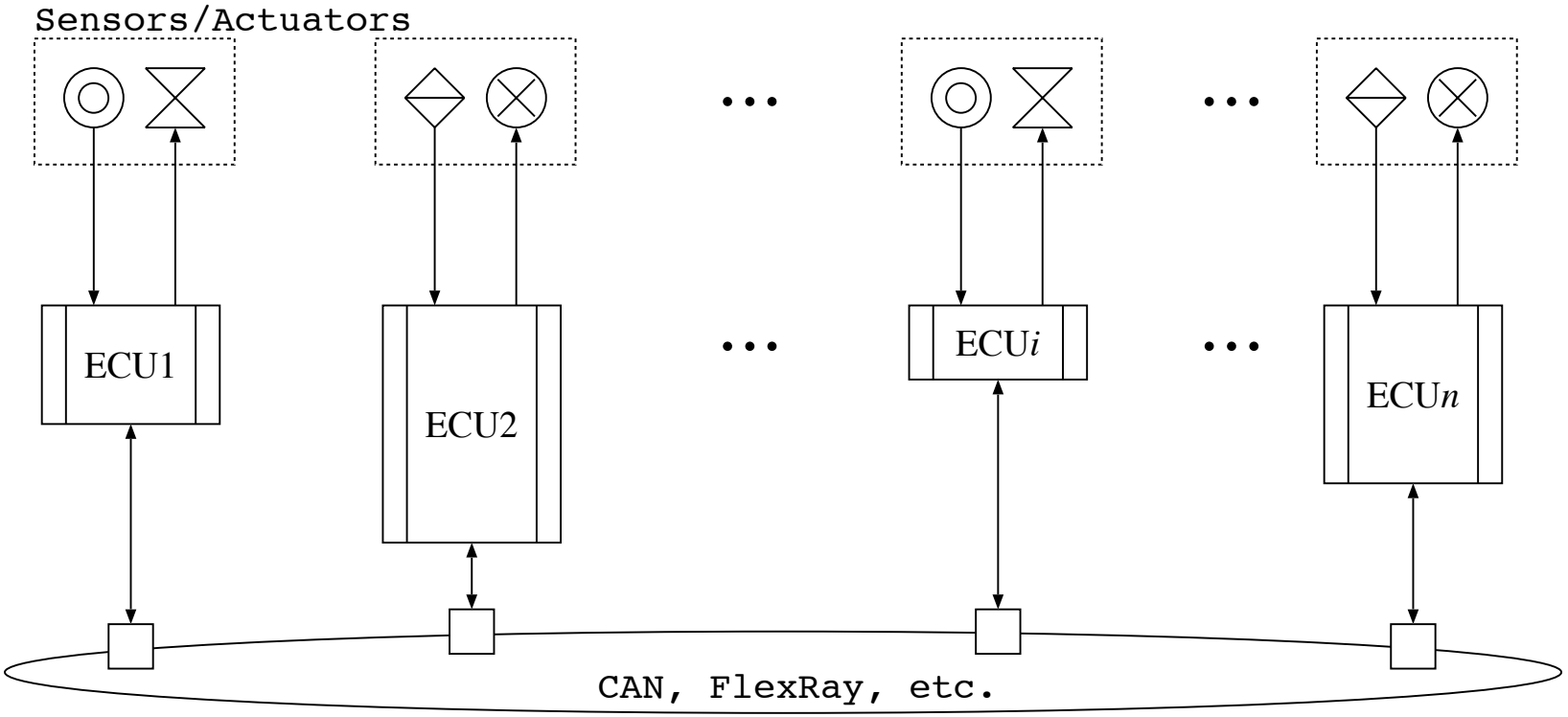
戦略的創造研究推進事業
「ディペンダブルVLSIシステムの基盤技術」

研究代表者　米田友洋（国立情報学研究所）
主たる共同研究者　今井　雅（弘前大学）
松本　敦（東北大学）
齋藤　寛（会津大学）

NII National Institute of Informatics 国立情報学研究所

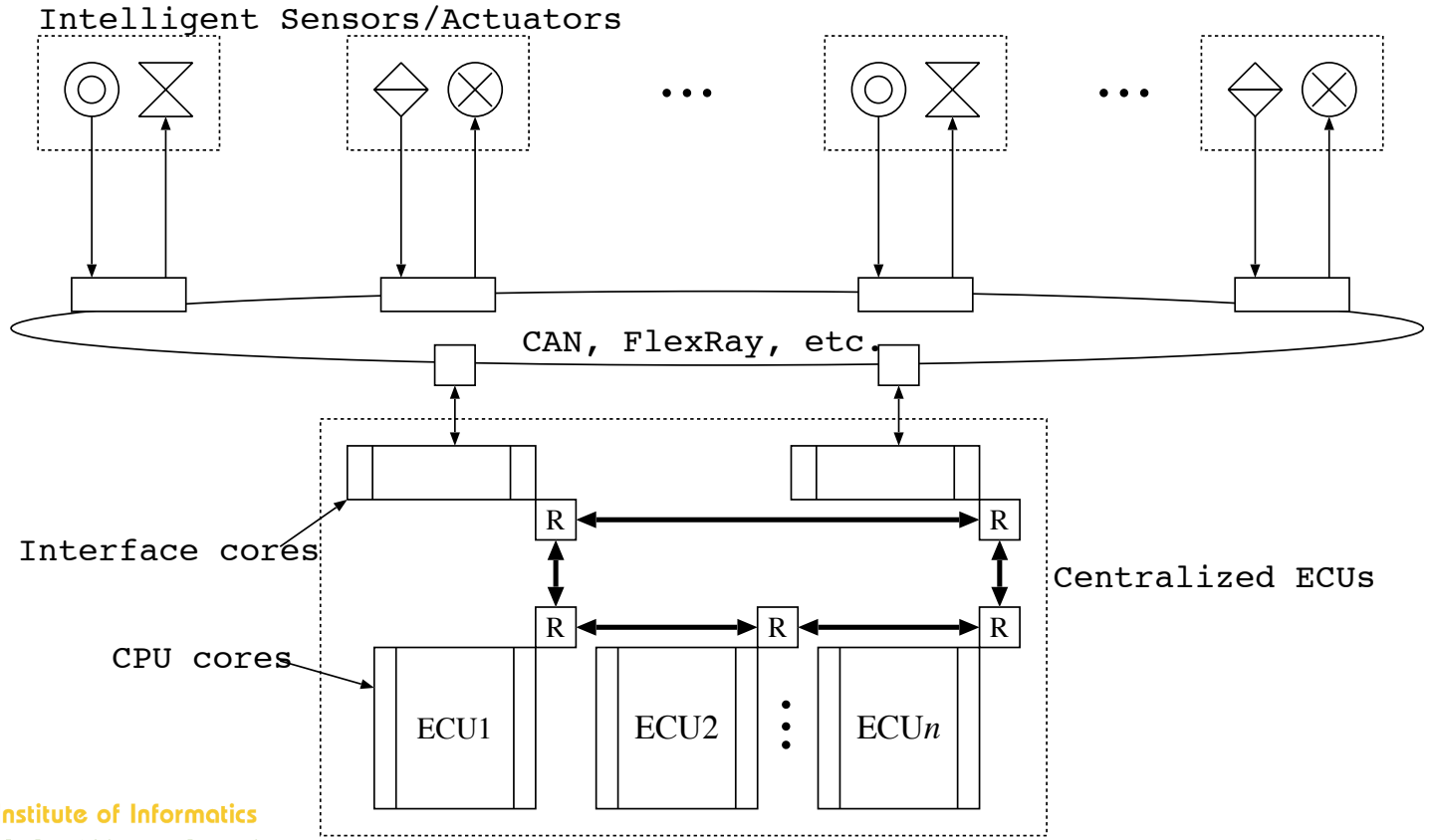
背景

- 近年の車には多くのECUが使われている
  - 従来のECU構成法



背景

- 近年の車には多くのECUが使われている
  - 集中型ECUのアプローチ



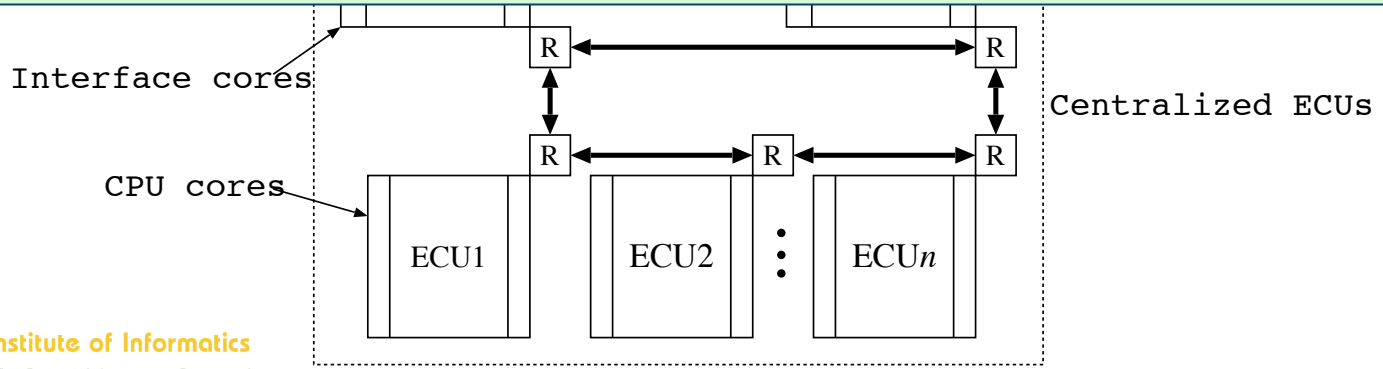
背景

- 近年の車には多くのECUが使われている
  - 集中型ECUのアプローチ

Intelligent Sensors/Actuators

どのECUもすべてのセンサ・アクチュエータにアクセス可

各ECUに、負荷に応じて効率よくタスクを割当できる
あるECUが故障しても、他のECUにタスクを振り分けることで、処理を実行可
（ECU故障により、そのECUに割当てられていた機能が失われることを回避可）



背景

- 集中型ECUアプローチ
  - NoC（ネットワークオンチップ）ベース
    - スケーラブルかつフレキシブル
    - いくつかのヨーロッパのプロジェクトで仮定
      - Recomp: Reduced certification costs for trusted multi-core platforms. *http://atc.ugr.es/recomp/.*
      - Race: Robust and reliant automotive computing environment for future ecars. *http://projekt-race.de/.*
  - マルチチップNoCベース

ISO 26262における指標

- Single-point fault metric

ASIL B	ASIL C	ASIL D
≥ 90%	≥ 97%	≥ 99%

- Latent-fault metric

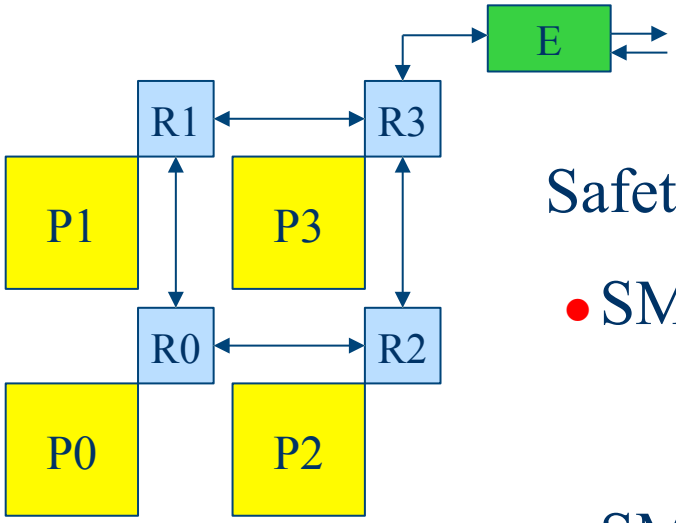
ASIL B	ASIL C	ASIL D
≥ 60%	≥ 80%	≥ 90%

- Probabilistic metric for random hardware failures

ASIL B	ASIL C	ASIL D
$< 10^{-7}$ 1/h	$< 10^{-7}$ 1/h	$< 10^{-8}$ 1/h

評価例

- NoCアプローチの簡単な例



Safety mechanisms

- SM1: 改良Pair & Swap方式
  [Imai,Yoneda DFT2011]
- SM2: 耐故障ルーティングアルゴリズム
  [Imai, Yoneda ASYNC2011]

Single-point fault metric

Element	Failure rate (fit)	Safety-related?	Failure mode	Distribution	Violate safety goal?	Safety mechanism	Diagnostic coverage	Residual or Single-point failure rate
P0～P3	1000	○	all	50%	○	SM1	99%	5
			all	50%	×			
R0～R3	100	○	all	50%	○	SM2	99%	0.5
			all	50%	×			
E	40	○	all	50%	○	none	0%	20
			all	50%	×			

SM1: 改良Pair & Swap方式
SM2: 耐故障ルーティングアルゴリズム

$$\left\{1-\frac{20+2+20}{4000+400+40}\right\}\times 100 = 99.1\% \qquad \text{(ASIL D)}$$

Latent fault metric

Element	Failure rate (fit)	Safety-related?	Failure mode	Distribution	Violate safety goal in combination with other failures?	Safety mechanism	Diagnostic coverage	Latent failure rate
P0～P3	1000	○	all	50%	○	SM1	100%	0
			all	50%	×			
R0～R3	100	○	all	50%	○	SM2	100%	0
			all	50%	×			
E	40	○	all	50%	×	none		
			all	50%	×			

SM1: 改良Pair & Swap方式
SM2: 耐故障ルーティングアルゴリズム

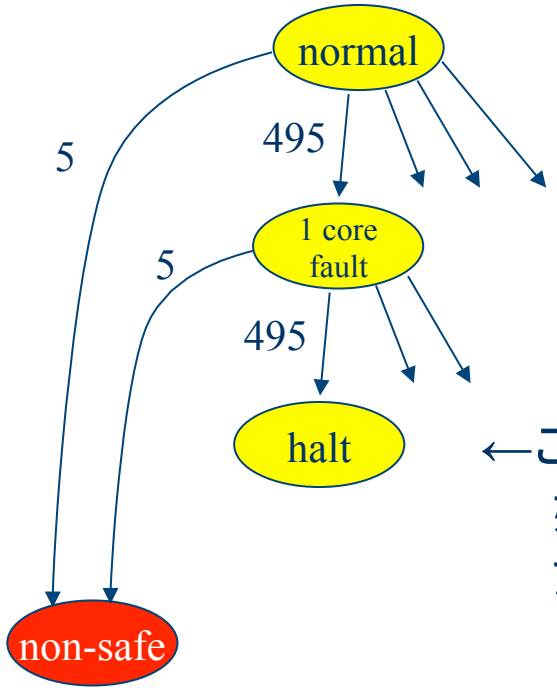
$$\left\{1-\frac{0}{4440-42}\right\}\times 100 = 100\% \qquad \text{(ASIL D)}$$

Probabilistic metric for random hardware failures

- $\omega_{all}=\omega_{core}+\omega_{network}+\omega_{ex}$
  - ω_{all} : 全システムの障害率
  - ω_{core} :コア部の障害率
  - $\omega_{network}$:オンチップネットワークの障害率
  - ω_{ex} :外部I/Oの障害率

Probabilistic metric for random hardware failures

- ω_{core}



ω_{core}=5 (fit)

2コアの故障まで耐えられる
3個目のコア故障で危険状態に遷移

↓

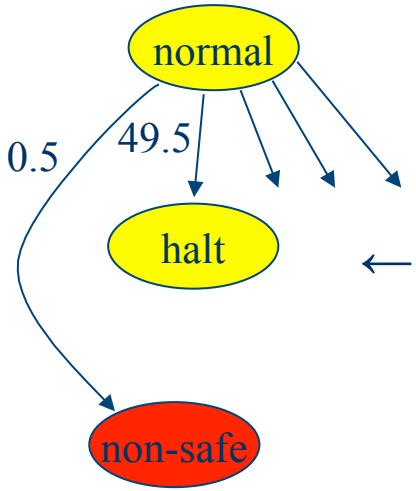
MTTFの改善にも寄与

←この時点（残り2台）で警告を出して
始動できないようにする。
ただし、動作中は2台で処理続行可能

Probabilistic metric for random hardware failures

- $\omega_{network}$

$\omega_{network}$=0.5 (fit)

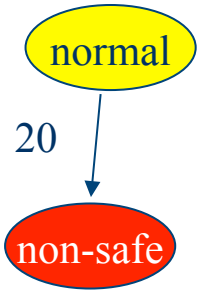


1つのルータまたはリンク故障に耐えられる
2つめの故障で危険状態に遷移
↓
MTTFの改善にも寄与

←この時点で警告を出して始動できないようにする。
ただし、動作中は処理続行可能

Probabilistic metric for random hardware failures

- ω_{ex}=20 (fit)



Safety mechanismなし

- ω_{all}=5+0.5+20=25.5 (fit)　ASIL　B or C
- ASIL Dを実現するためには、少なくとも外部I/Oの多重化が必要