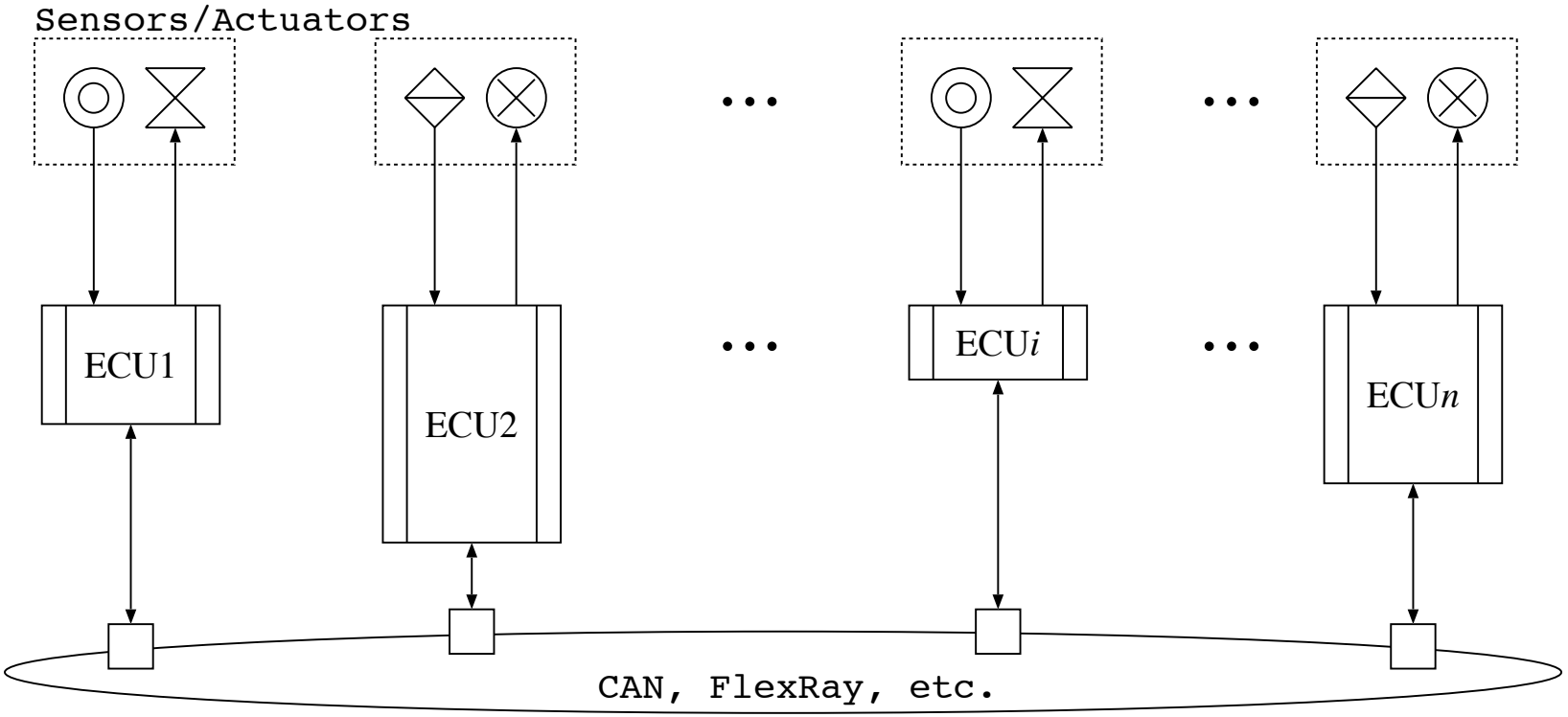
Multi-Chip NoC Approach for Automotive Applications

Tomohiro Yoneda (National Institute of Informatics)
Masashi Imai (Hirosaki University)
Atsushi Matsumoto (Tohoku University)
Hiroshi Saito (University of Aizu)

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

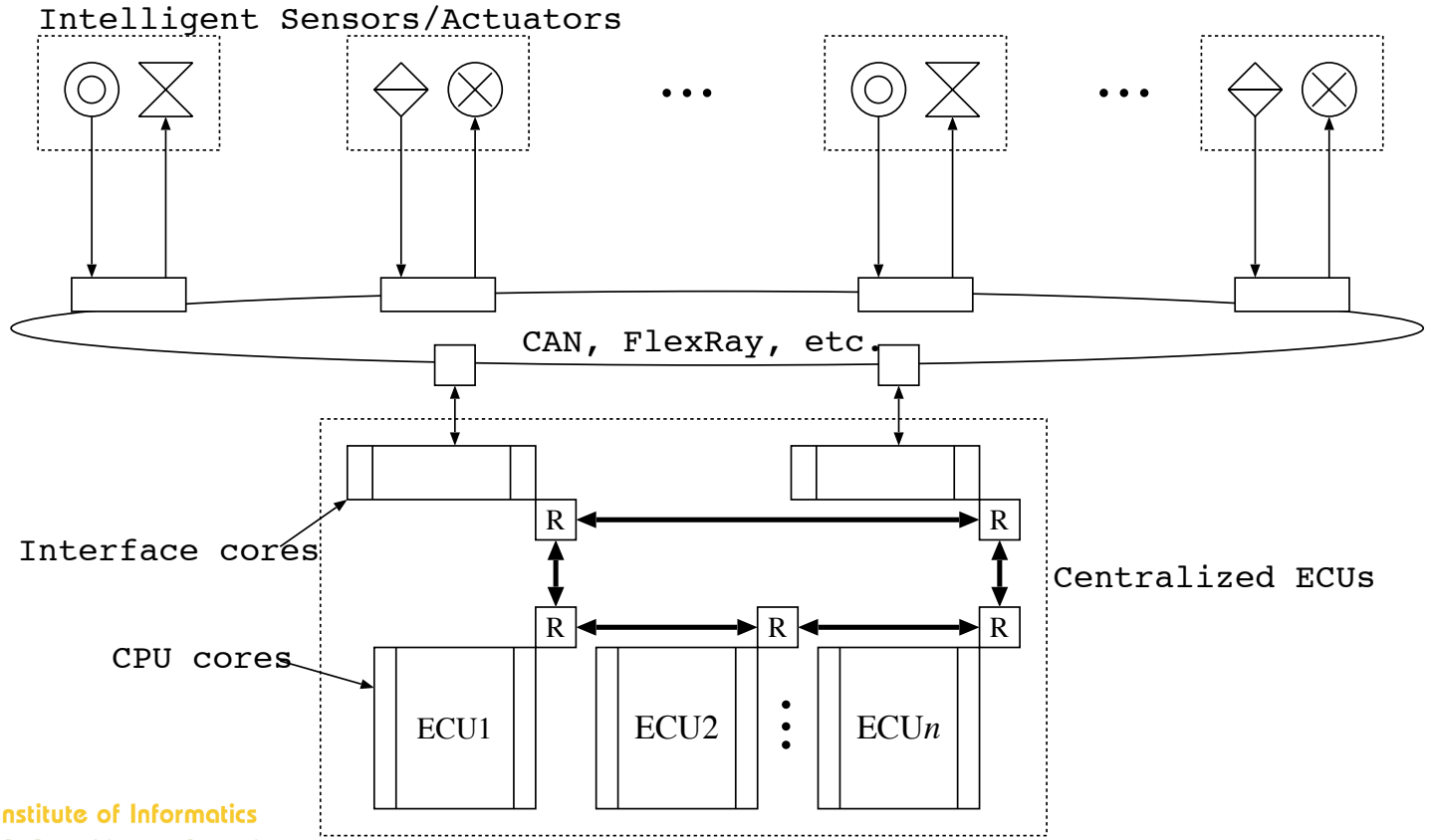
Backgrounds

- Recent automobiles are equipped with many ECUs
  - Conventional ECU configuration



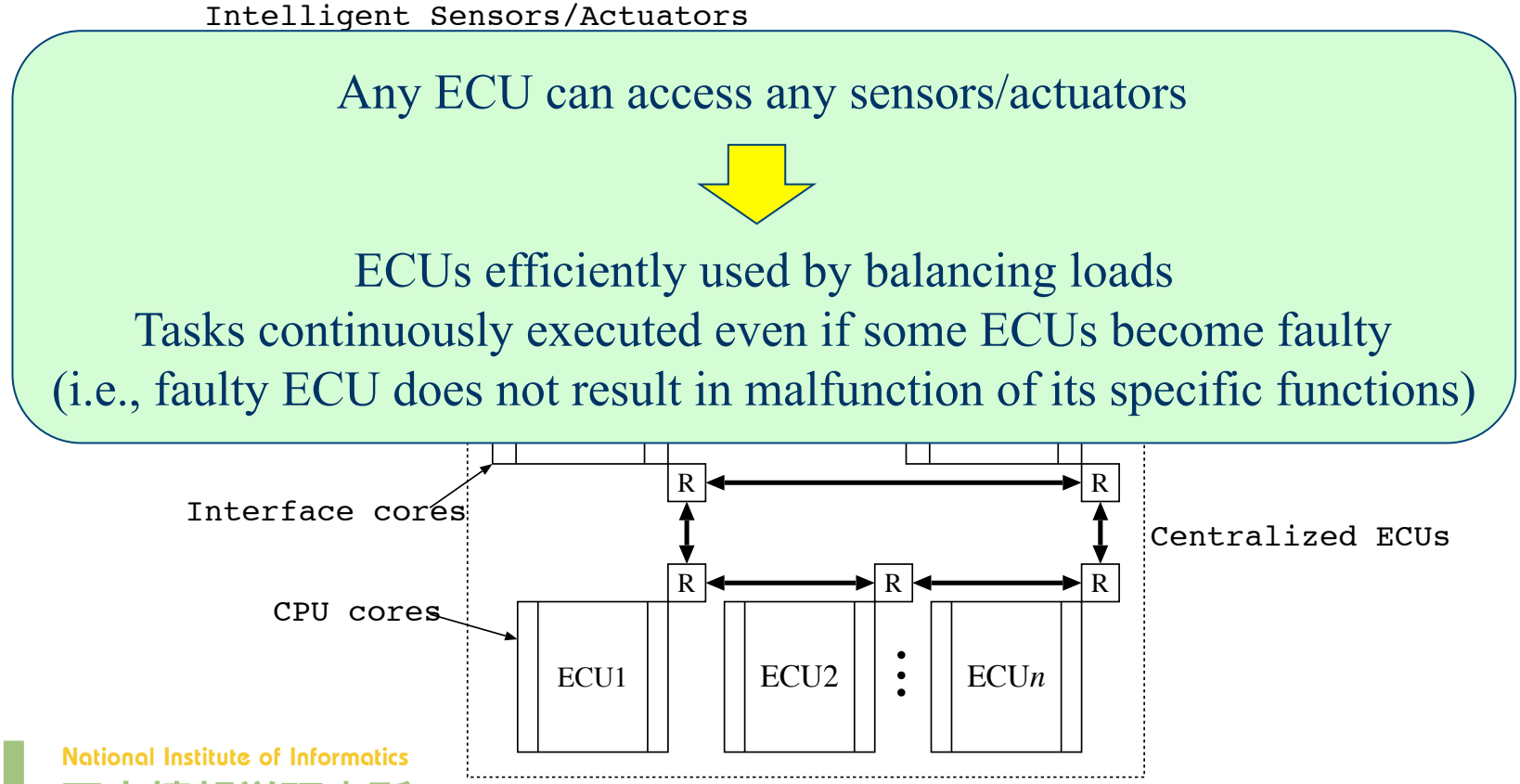
Backgrounds

- Recent automobiles are equipped with many ECUs
  - Centralized ECU approach



Backgrounds

- Recent automobiles are equipped with many ECUs
  - Centralized ECU approach



Backgrounds

- Centralized ECU approach
  - NoC (Network-on-Chip) based
    - Scalable and flexible
    - Some European projects
      - 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/.*
  - Multi-Chip NoC based

Metrics in ISO 26262

- Single-point fault metric

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

- Latent-fault metric

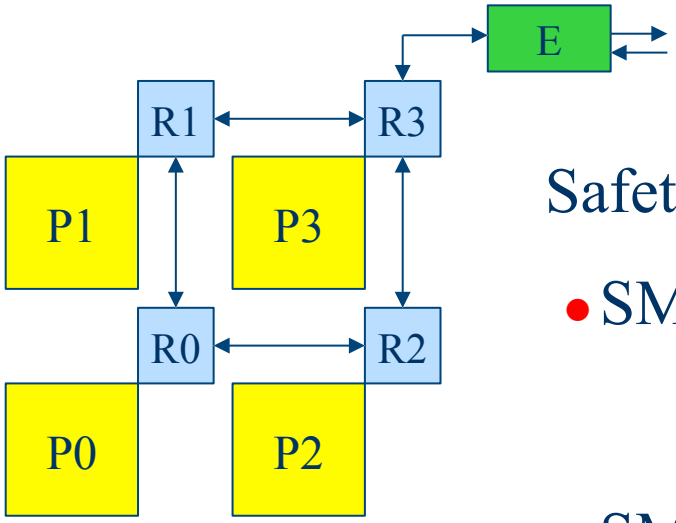
ASIL B	ASIL C	ASIL D
≥ 60%	≥ 80%	≥ 90%

- Probabilistic metric for random hardware failures

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

Trial to evaluate metrics

- Simple example based on our NoC approach



Safety mechanisms

- SM1: Modified Pair & Swap method [Imai,Yoneda DFT2011]
- SM2: Dependable Deadlock-free routing [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: Modified Pair & Swap
SM2: Dependable routing algorithm

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

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: Modified Pair & Swap
SM2: Dependable routing algorithm

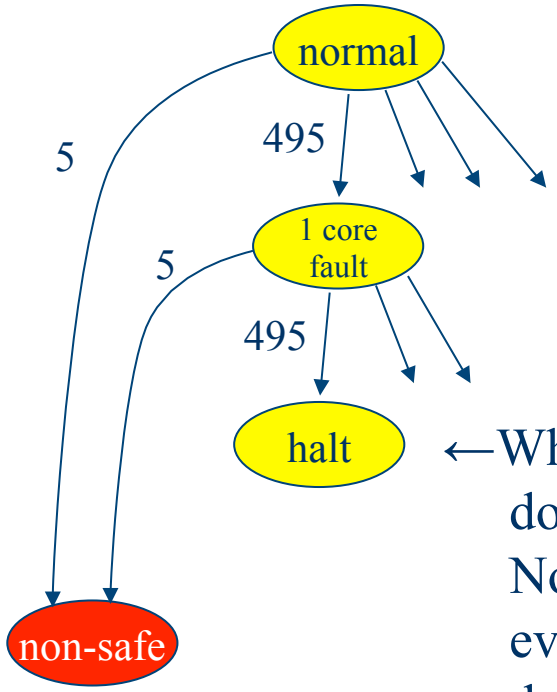
$$\left\{1-\frac{0}{4440-42}\right\}\times 100 = 100\% \qquad \text{(ASIL D)}$$

Probabilistic metric for random hardware failures

- $\omega_{all}=\omega_{core}+\omega_{network}+\omega_{ex}$
  - ω_{all} : Failure rate of the whole system
  - ω_{core} : Failure rate of the cores
  - $\omega_{network}$: Failure rate of the on-chip network
  - ω_{ex} : Failure rate of the external IO

Probabilistic metric for random hardware failures

- ω_{core}



ω_{core}=5 (fit)

Tolerate up to two faulty cores,
i.e., third fault leads to non-safe state

⇩

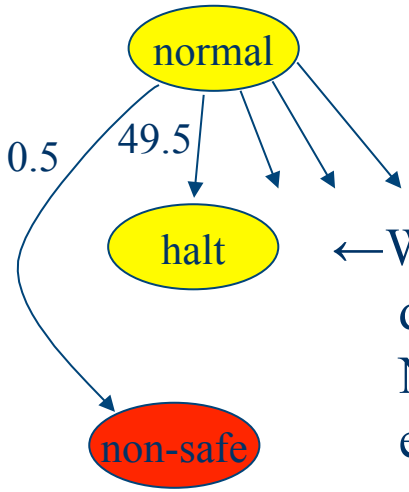
Contribute to longer MTTF

←When 2 cores are down, the detection mechanism does not allow to start up the system again.
Note that the system can continue to work correctly, even if the second core becomes faulty during the operation.

Probabilistic metric for random hardware failures

- $\omega_{network}$

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



Tolerate a router or link fault,
i.e., second fault leads to non-safe state

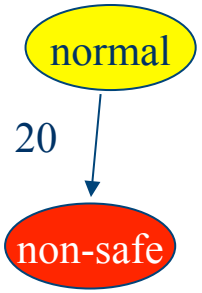
⇓

Contribute to longer MTTF

←When a router or link is down, the detection mechanism does not allow to start up the system again.
Note that the network can continue to work correctly, even if a router or link becomes faulty during the operation.

Probabilistic metric for random hardware failures

- ω_{ex}=20 (fit)



No safety mechanism

- ω_{all}=5+0.5+20=25.5 (fit) ASIL B or C
- For ASIL D, some safety mechanism of external IO is at least needed