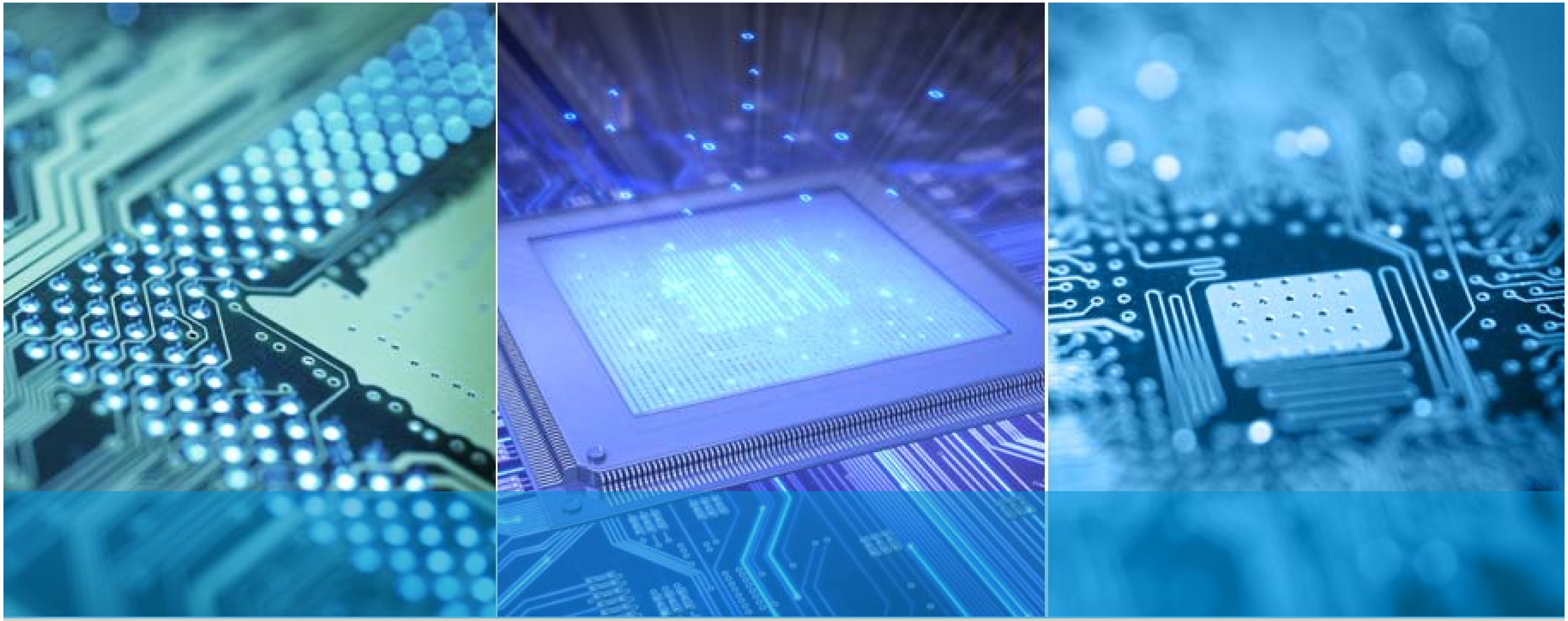


September 11, 2009

Reliability Requirements for Automotive

Tony Reipold, Kevin Kemp, Claude Moughanni
Freescale Semiconductor

Reliability Requirements for Automotive

- Market Characteristics
- Safety Standards
- Research Needs /Discussion Points

Market Characteristics

- Automotive reliability needs driven by
  - Consumer expectation: JD Power, Consumer Reports …
  - Warranty / service / recall cost
  - Liability, litigation, regulatory
- Automotive electronics growth - Competitive new features
  - Powertrain: Engine control, transmission, instrumentation
  - Chassis / safety: ABS, ESC, active suspension, airbag …
  - Body electrical: Door, window, lock, alarms …
  - Comfort / convenience: Climate control, memory seat …
  - Energy efficiency: Hybrid, EV, electric steering (weight reduction) …
  - Infotainment, telematics
  - Driver aid: Radar, night vision, lane departure, active cruise …
  - Intelligent highway, autonomous vehicle …
- Risk averse
  - Long technology adoption cycles
- Operating Environment
  - Temperature (-40 to 175ºC), moisture, vibration, EM noise
- Extreme Cost Sensitivity

Reliability Threats

- Device wear-out (hard fail or degradation)
- Manufacturing defects (test escapes)
- HW and SW design errors (verification escapes)
- Transient faults (alpha particles, cosmic rays, noise, EMI)
- Overstress failure (ESD, power surge, short circuit load)
- Parametric variability (performance marginality, increased failure susceptibility)
- Analog and sensor components as well as digital
- Over reaction to transient or correctable faults (unnecessary system shut down)
- Improper maintenance

Basic Concepts and Taxonomy of Dependable and Secure Computing A. Avizienis et. al., IEEE Trans on Dependable and Secure Computing, 2004

Safety Systems versus Safety-Critical Systems

		Functional safety	
		Non-safety critical [failure $\Rightarrow$ no imm. danger]	Safety-critical [failure $\Rightarrow$ immediate danger]
Automotive Safety Systems	Active Safety [avoid accident]	Braking Assistant	ESP
	Passive Safety [survive accident]	Safety Belt Pretensioner	Airbag
Non-Safety Systems		Lighting	Electronic Throttle Control

⇨ Functional Safety is a property rather than an application domain
⇨ many automotive systems require this property
⇨ differences in criticality and moment of activation

freescale™ semiconductor

Safety Standards

IEC 61508

- General safety standard for E/E/PE systems
- First edition 2000
- Metrics:
  - Probability of dangerous failure per hour (PFH)
  - Safe Failure Fraction (SFF)
- 4 Safety Integrity Levels (SIL)
- Hardware redundancy in formulas (HFT)

	SIL 1	SIL 2	SIL 3
PFH [1/h]	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$
SFF	>=60%	>=90%	>=99%

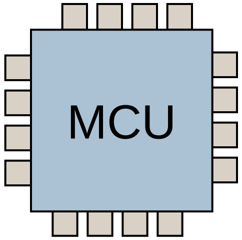
Note: specialised table for typical automotive application with HFT=0

ISO 26262

- Adaption of IEC 61508 for the automotive industry
- First edition emerging now
- Metrics:
  - Probability of violation of safety goals (PFH)
  - Single Point Fault Metric (SPFM)
  - Latent Fault Metric (LFM)
- 4 Automotive SILs (ASIL)
- Hardware redundancy in structural modeling

	ASIL B	ASIL C	ASIL D
PFH [1/h]	$<10^{-7}$ (recom.)	$<10^{-7}$	$<10^{-8}$
SPFM	>90%	>97%	>99%
LFM	>60%	>80%	>90%

Deriving MCU Safety Level Measures

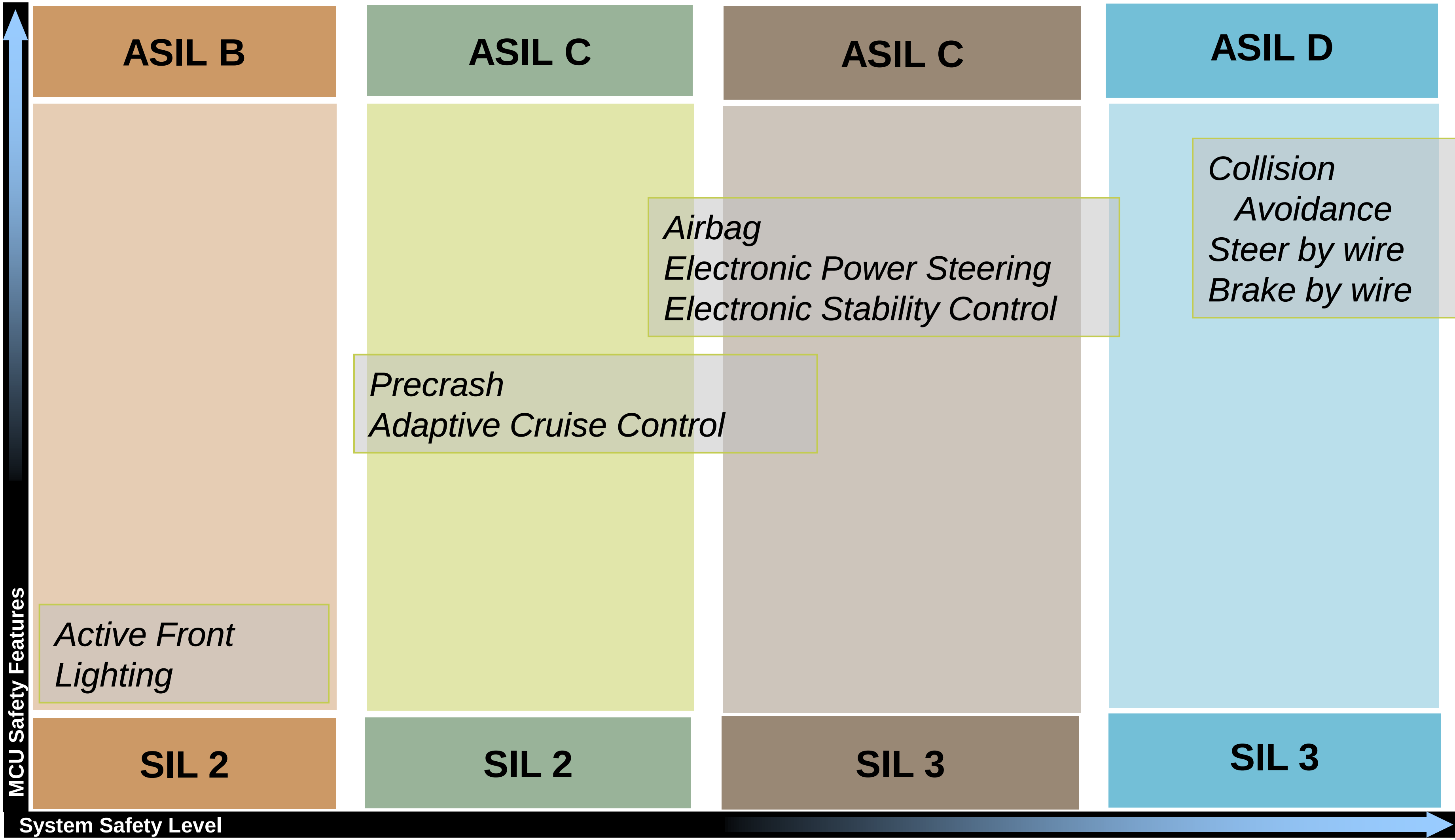


- Self test measures
  - Ensure that the device is free from dormant faults
  - Core self-test
  - Device self-test
- Error detection measures
  - Stop errors from propagating beyond component boundary
    - Error correction (compensation)
    - Shut down (fail-silent)
  - HW plausibility based
    - Illegal address/op-code detection, Supervisor & user modes, memory error detection, ECC, clock monitors, voltage supervision, watchdogs,
  - HW redundancy based
    - redundant peripherals, dual-core
- Development process measures
  - Avoid systematic failures
  - Follow IEC 61508 process requirements

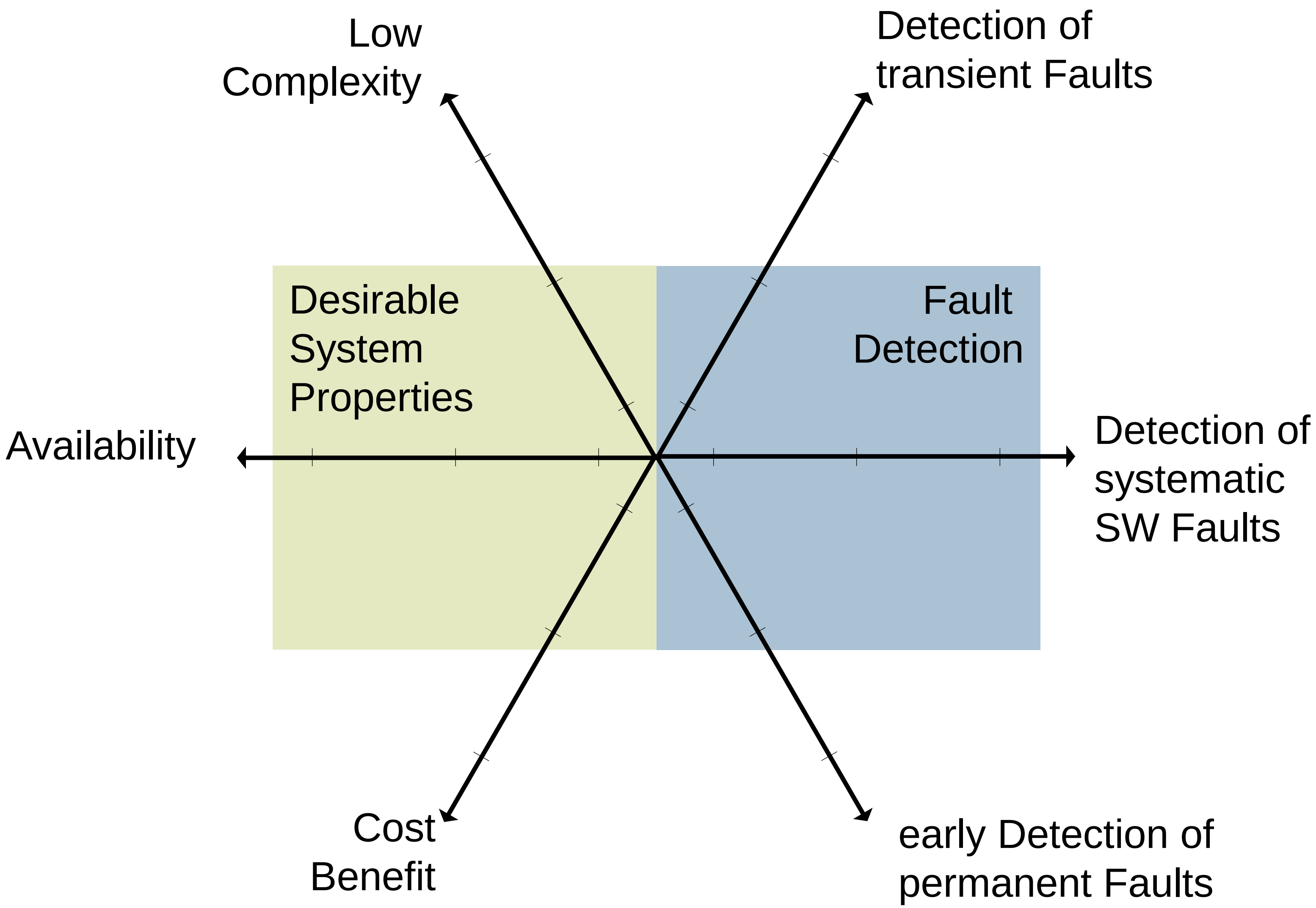
Fault Tolerance/Resiliency Techniques

	Device	Circuit / uArch	System Arch	Firmware / Driver / OS	Application SW
Guardbanding / Uprating / Overdesign	x	x	x		
Fail-over machanisms (e.g ABS)					
Communication channel coding (ECC)		Low cost / very effective			
Memory Error Correction		low to med cost / very effective			
Self-checking digital circuits (Error correcting buses and logic) Self-Checking and Fault-Tolerant Digital Design, Parag K. Lala; Academic Press, 2001					
Triple modular redundancy + voting (TMR)			Very high cost / very effective		
Hardware replicate / diversity + checker			Med to high cost / effective		
Software diversity + checker					High cost
On line BIST http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04700583		X (memory/logic)	x	x	
Checkpoint – test – recover (BulletProof Silicon - Austin/Bertacco) http://www.eecs.umich.edu/~taustin/papers/dtco-25-04-aust.pdf http://www.eecs.umich.edu/~taustin/papers/HPCA06-bullet.pdf		x		x	
Asymmetric reliability - control vs. data (ERSA – Mitra) http://selse3.selse.org/Papers/17_Bau_P.pdf			x		
Monitors / diagnostics (Clock source/quality monitors, open/short circuit tests, cpu tests, voltage/current monitors, multiple A2D test voltages)		Low cost / effective	x		
NoC w. redundancy + resilient routing			x		
On-chip sensors (thermal, NBTI, TDDB …)	x			x	
Selective component hardening based on criticality (VGER - Seshia)	x				

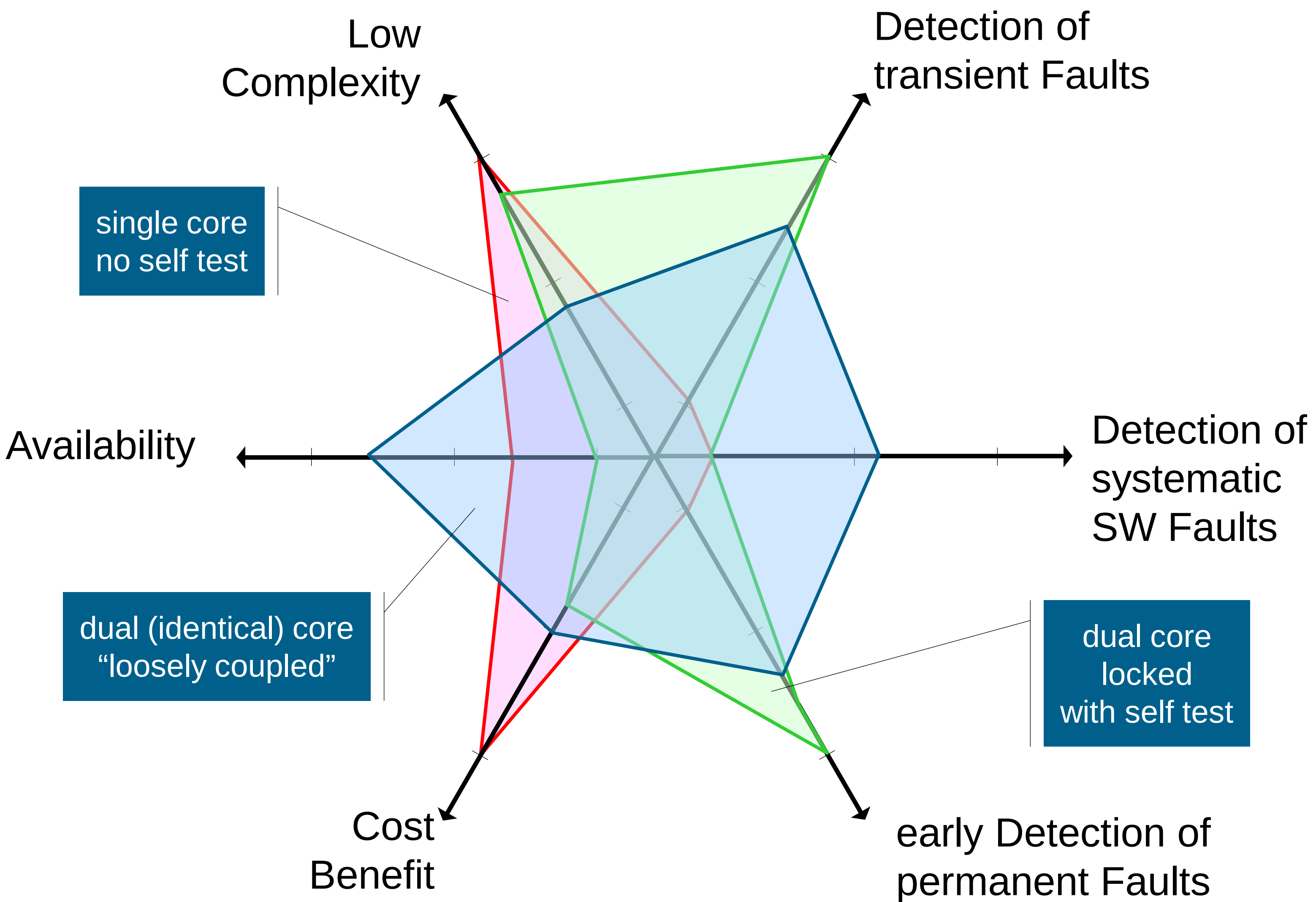
Chassis / Safety Applications



Metrics for Fault Tolerance Mechanisms



Fault Tolerant Architectures



Automotive System Level Example

Implementation Abstraction	Example Application (for Illustration)		
Application SW	Auto Drive Vehicle: Integrate all data sources and control direction and speed		
Firmware / Driver / OS	Read road sensors	Read car radar	GPS, direction, speed, Etc
System / Interfaces	Communicate sense results	Communicate radar results	
Board / Subsystem	Sensor to control logic	radar to control logic	
Packaged IC / Sensors	Sensor with lens/package	radar with package	
Manufacturing / Device	Manufacture sensor	Manufacture radar x/r	

System level goals:

- Optimize total system resilience and cost
- Optimize component level resilience and cost in context of a the system
- Compare alternate and innovative architectural solutions
- Use tools to enable accurate modeling, repeatable processes and faster time to market.
- Tools should cover system requirements capture phase through product delivery

Resilient system design requires cross layer and within layer communication of :

- Failure occurrence
- Recovery implemented
- Probability of failure recurrence
- Distance from lowest allowable safety critical degraded mode

Research Needs / Discussion Points

- Requirements capture and architecture exploration methodology & tools
- New, low cost resilient architectures / methods
  - Apply to “mature” technologies to achieve very high reliability levels
- Software resiliency
  - Software (faults) are part of the problem
  - Software (may be) part of the solution
- Provable compliance (SIL / ASIL) of fault tolerant designs
  - At the system level
  - At each level in the system
  - Design, manufacturing, HW, SW, power supply, packaging, documentation…
  - Cross discipline resiliency models
- Commonalities with Aerospace (- rad hard, + low cost)
  - Life-critical applications
  - Conservative / risk-averse
  - Application follower (dynamics, navigation telematics,, autonomy …)
- Communication and interfaces
  - Unambiguous system communication within a level and across levels
  - Optimized local communication overhead requirements (cost optimization)
  - Resilient interfaces

freescale™ semiconductor