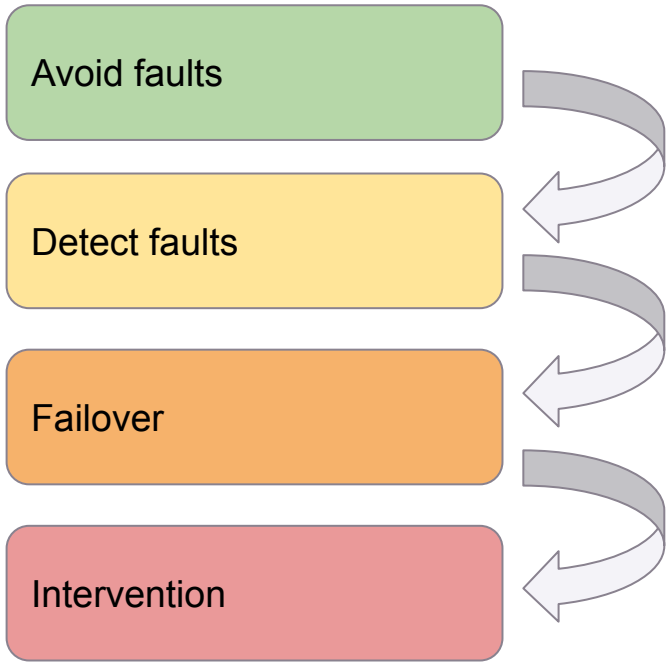
25: Safety Standards

Milestone demo reminders

- Just one slide (project description and goals)
- Brief (5 min) demo
- Half of the groups on Monday, half on Wednesday
  - Randomly assigned, will announce by end of today
- We will ask for your FSM and slide so that it can be peer-reviewed by others

Review: escalation of safety



Safety standards

Guide how to engineer for safety

- How to assess risk
- What SW processes to use
- What code standards to follow
- How much/what kinds of testing
- How much formal verification

Different standards for different domains

- Progression for automotive: MISRA -> IEC 61508 → ISO 26262 →SOTIF/ISO21448 (→UL 4600?)

Risk Matrices

A way of reasoning about the amount of risk of a hazardous event

IEC 61508		Consequence			
Likelihood (failures per year)		Catastrophic Multiple loss of life	Critical Single loss of life	Marginal Major injuries	Negligible Minor injuries at worst
Frequent	$> 10^{-3}$			I	II
Probable	10^{-3} - 10^{-4}			II	III
Occasional	10^{-4}-10^{-5}	I		III	III
Remote	10^{-5}-10^{-6}	II			IV
Improbable	10^{-6}-10^{-7}	III			
Incredible	$< 10^{-7}$	III	IV	IV	

Unacceptable

Undesirable

Tolerable (cost tradeoff)

Acceptable

Tell your neighbor about the cautionary tale you researched (Boeing 737, Stuxnet, Ariane 5, SmartHue Lightbulbs, Radiology Password, ConnMan)

Where would you put this system on a risk matrix (what was the consequence/potential consequence? What *should* the probability be?)

IEC 61508		Consequence			
Likelihood (failures per year)		Catastrophic	Critical	Marginal	Negligible
		Multiple loss of life	Single loss of life	Major injuries	Minor injuries at worst
Frequent	$> 10^{-3}$	I	I	I	II
Probable	10^{-3} - 10^{-4}	I	I	II	III
Occasional	10^{-4}-10^{-5}	I	II	III	III
Remote	10^{-5}-10^{-6}	II	III	III	IV
Improbable	10^{-6}-10^{-7}	III	III	IV	IV
Incredible	$< 10^{-7}$	III	IV	IV	IV

Unacceptable

Undesirable

Tolerable (cost tradeoff)

Acceptable

The burns suffered by Patricia Anderson and her family when their elderly Chevrolet Malibu was hit by another car on Christmas eve in 1993 were real and horrific. The car, whose fuel tank General Motors had put close to the bumper, exploded, leaving three passengers with burns over more than 60% of their bodies. So when a Californian jury awarded damages against GM, it was not the degree of harm that attracted startled comment, but the scale of the award—an astonishing $4.9 billion.

The firm was not allowed to reveal to the jury that the driver of the other car was drunk, or to talk about the good safety record of the Malibu. Instead the case centred on a cost-benefit analysis written in 1973 by a GM engineer. After assigning a $200,000 value to a human life, Edward Ivey estimated that it would cost $2.40 per car to settle lawsuits resulting from any deaths, as compared with $8.59 to fix the fuel-tank problem.

Article source: Economist, July 17 1999
Image source

Safety Integrity Levels

A (standards-based) target to attain for each safety function

Named SIL levels (IEC 61508/ISO 26262 has SIL-1, SIL-2, SIL-3, SIL-4)

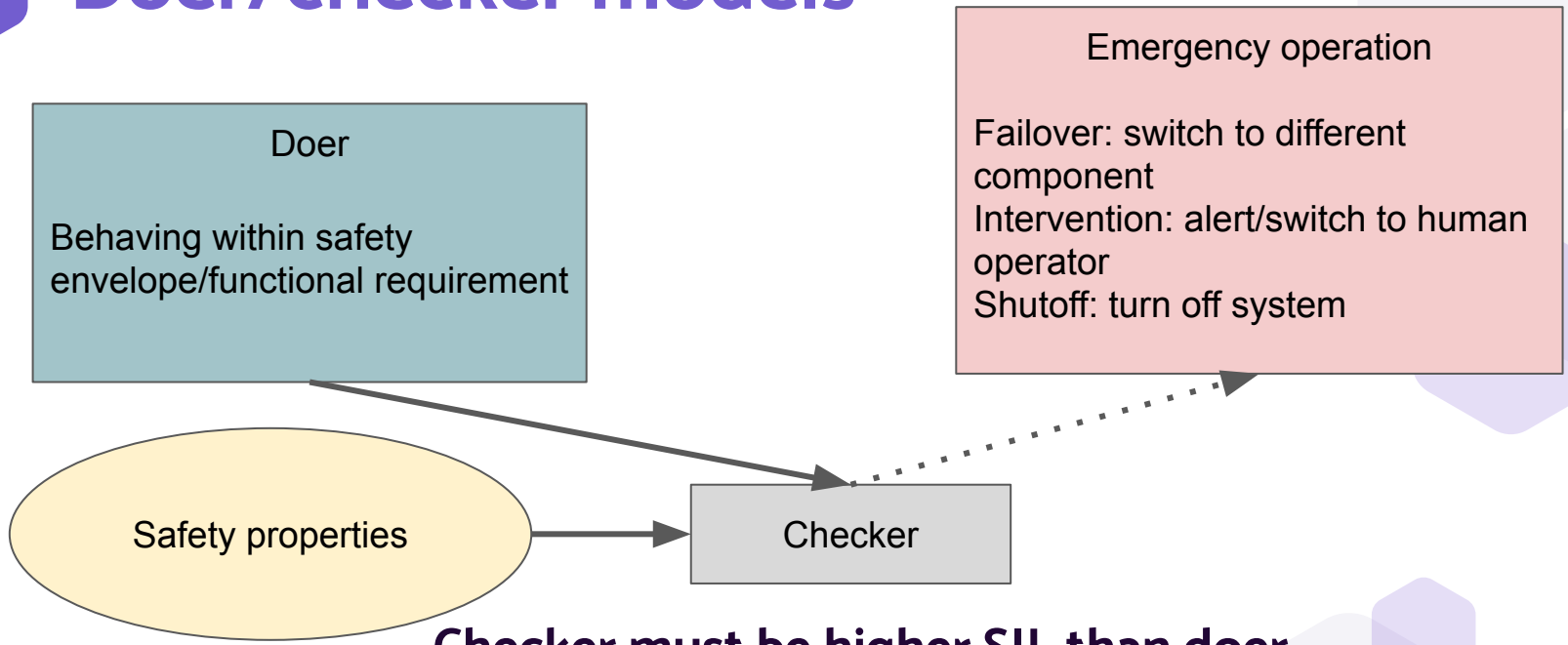
- SIL-4 means least acceptable failures (in ISO26262, $< 10^{-9}$ per hour)

Each SIL may require:

- Maximum accepted risk of failure
- Minimum accepted software quality
- Minimum accepted redundancy architecture
- All hardware to be certified at or above that level

} Analysis and mitigation techniques

Doer/checker models

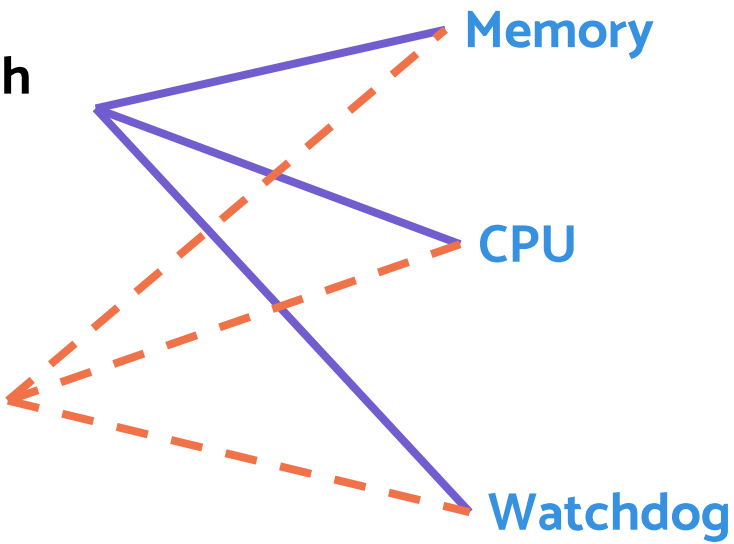


Checker must be higher SIL than doer
Must be confident detection/emergency operation won't fail

Mixed-SIL Interference

Critical task (high SIL)

Non-critical task (low SIL)



Different standards for different domains

Approximate cross-domain mapping of ASIL

Domain	Domain-Specific Safety Levels					
Automotive (ISO 26262)	QM	ASIL-A	ASIL-B	ASIL-C	ASIL-D	-
General (IEC 61508)	-	SIL-1	SIL-2		SIL-3	SIL-4
Railway (CENELEC 50126/128/129)	-	SIL-1	SIL-2		SIL-3	SIL-4
Space (ECSS-Q-ST-80)	Category E	Category D	Category C		Category B	Category A
Aviation: airborne (ED-12/DO-178/DO-254)	DAL-E	DAL-D	DAL-C		DAL-B	DAL-A
Aviation: ground (ED-109/DO-278)	AL6	AL5	AL4	AL3	AL2	AL1
Medical (IEC 62304)	Class A	Class B			Class C	-
Household (IEC 60730)	Class A	Class B			Class C	-
Machinery (ISO 13849)	PL a	PL b	PL c	PL d	PL e	-

Image source

Standards inform practice

ISO 26262

Table 3: 7.4.3 Principles for software architectural design		ASIL A	ASIL B	ASIL C	ASIL D
1a	Hierarchical structure of software components	++	++	++	++
1b	Restricted size of software components [a]	++	++	++	++
1c	Restricted size of interfaces [a]	+	+	+	+
1d	High cohesion within each software component [b]	+	++	++	++
1e	Restricted coupling between software components [a, b, c]	+	++	++	++
1f	Appropriate scheduling properties	++	++	++	++
1g	Restricted use of interrupts [a, d]	+	+	+	++

Table 4: 7.4.14 Mechanisms for error detection at the software architectural level		ASIL A	ASIL B	ASIL C	ASIL D
1a	Range checks of input and output data	++	++	++	++
1b	Plausibility check [a]	+	+	+	++
1c	Detection of data errors [a]	+	+	+	+
1d	External monitoring facility [c]	o	+	+	++
1e	Control flow monitoring	o	+	++	++
1f	Diverse software design	o	o	+	++

Image source

Use of standards

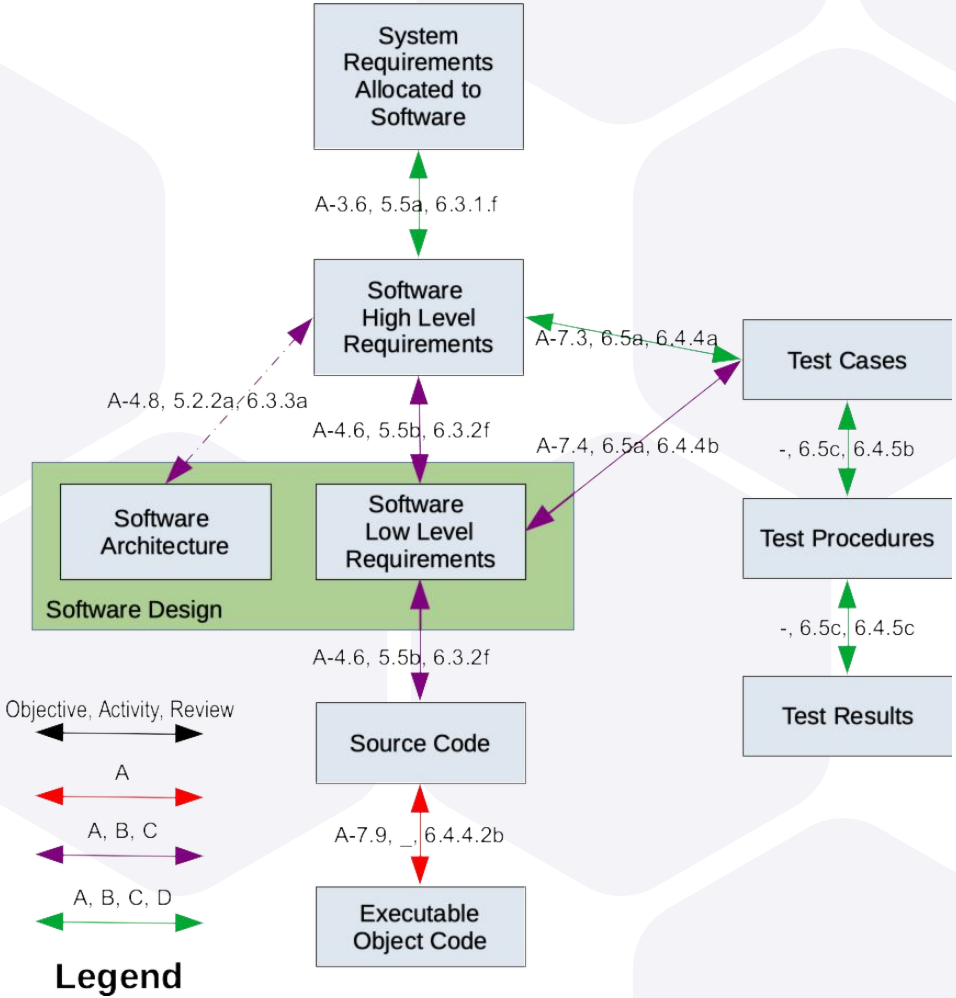
FPGAs (IEC 61508) vs. Airplanes (DO-178C)

Microchip functional safety page FAA software approval guidelines NHSTA study of safety standards

Serial Number	Objectives	Software Level-A	Software Level-B	Software Level-C	Software Level-D
1	Software Code complies with low-level requirements.	Applicable	Applicable	Applicable	Not Applicable
2	Source Code complies with software architecture.	Applicable	Applicable	Applicable	Not Applicable
3	Source Code is Verifiable.	Applicable	Applicable	Not Applicable	Not Applicable
4	Source Code conforms to standards.	Applicable	Applicable	Applicable	Not Applicable
5	Source Code is traceable to low-level requirements.	Applicable	Applicable	Applicable	Not Applicable
6	Source Code is accurate and consistent.	Applicable	Applicable	Applicable	Not Applicable
7	Output of software integration process is complete and correct.	Applicable	Applicable	Applicable	Not Applicable
8	Parameter Data Item File is correct and complete.	Applicable	Applicable	Applicable	Applicable
9	Verification of Parameter Data Item File is achieved.	Applicable	Applicable	Applicable	Not Applicable

DO 178C Table A-5: Verification of Outputs of Software Coding and Integration Process

Image source



[Image source]

Should cars be engineered to the same safety standards as planes?

- *Same rigor?*
- *Legal requirement?*