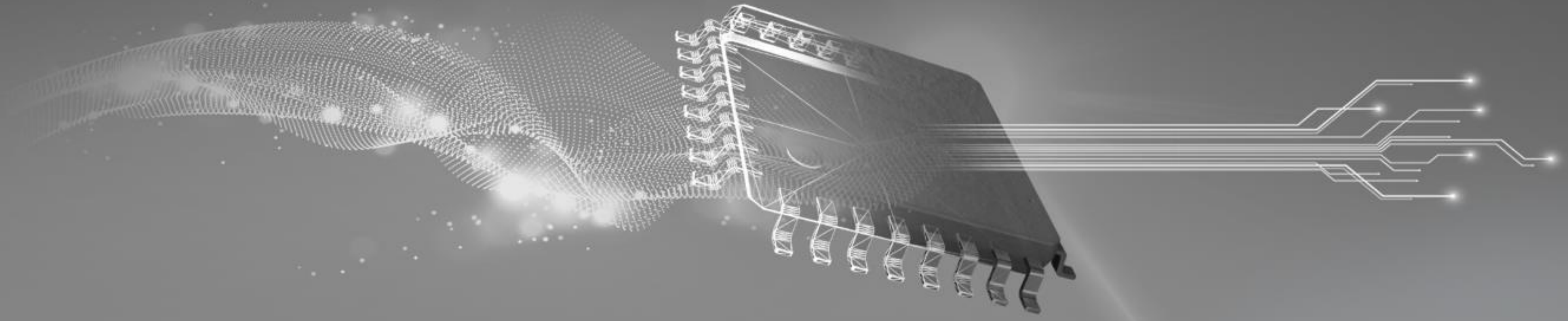
TI TECH DAYS



Be confident around automotive functional safety

Tomas Urban

Systems Engineering - Automotive Powertrain Systems

Presentation summary

Session summary:

Many automotive systems are related to functional safety. Offering a functional safety expertise becomes an important door-opener and ultimately a selling point. This is an introductory presentation to those who want to get a starting point for functional safety communication with customers.

What you'll learn:

- What most important terms, acronyms and concepts are worth to know?
- What actually is an ASIL rating? Who and how are safety goals classified with ASIL rating?
- Update on how are the HW components classified and how does it match with TI's portfolio.

Agenda

- Functional safety (FS)
- Risk quantification
- ASIL (SIL)
- Safety goal
- FIT/MTBF/λ
- FIT rates
- Safety mechanism, diagnostic coverage, FMEDA
- HW metrics & HW development
- FS development iterative example
- HW components

Functional safety

- Functional safety is the absence of *unreasonable risk* due to hazards caused by *malfunctioning behavior* of E/E systems
- Managing (reducing) the risks associated with function of a system (transportation, machinery, medical…)
- Both FS and FuSa acronyms are used

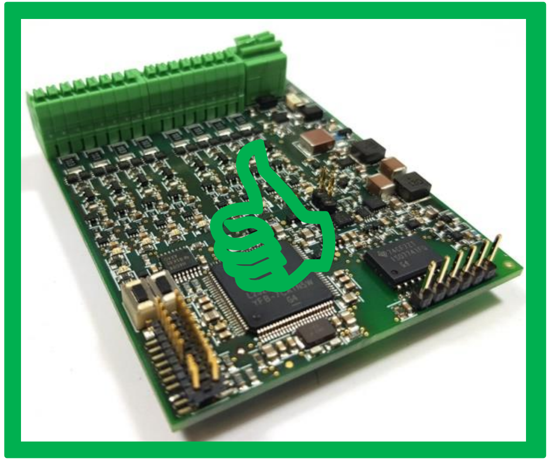
HW

- Random HW capability → HW metrics :
  - SPF
  - LFM
  - PMHF

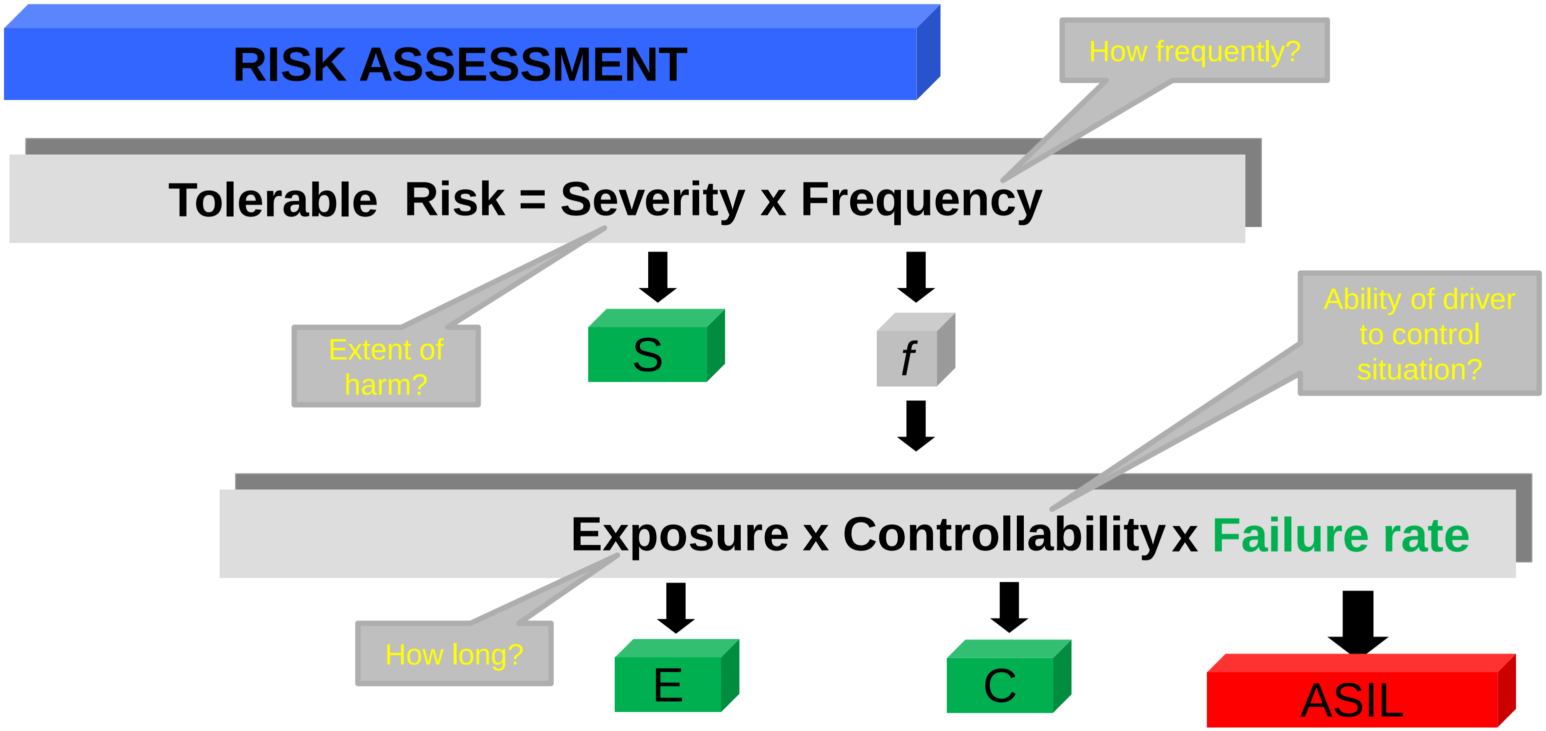
  (more on that later)
- Systematic capability → Rigorous development, traceability, supporting processes

SW

- Systematic capability *only* → Rigorous development, traceability, supporting processes



Risk quantification using “E”, “S”, “C”



Original slide credit: Bharat Rajaram

ASIL: **A**utomotive **S**afety **I**ntegrity **L**evel

ASIL (SIL)

- Outcome from classification of a ***hazardous event*** e.g. ***"Fire"***
  - Specified for vehicle situation or operation mode of the vehicle e.g. ***"The vehicle is stationary"***
  - Classification: ***ASIL A, B, C, D***
  - Result of evaluation of of ***S,E,C*** (from previous slide)
- ASIL classification then translates down to the system architecture into ***Safety goals***
- Specifies
  - Methods for system development
  - HW metrics (more on that later)
  - Verification and validation techiques

Safety goal

Assessment of hazards and risks result in definition of Safety goals and their ASIL classification.

- Safety goal is top level safety requirement
- Typically includes some time interval
- Formulation like:

” Unintended activation of the airbag is prevented (ASIL D)”

FIT / MTBF / λ

- Sometimes confusing and all used in the same context.
- All are values derived from statistics and probability
- FIT = number of **F**ailures **I**n **T**ime interval of 10^9 hours of operation
- MTBF =in hours stands for **M**ean **T**ime **B**etween **F**ailures.
  For non-repairable systems (e.g. electronic components) the meaning is MTTF (**M**ean **T**ime **T**o **F**ailure)
- λ in $hours^{-1}$ = a failure rate (number of failures in one hour)

Example of FS FIT rates acc. to SN29500

Component type	FIT
Resistors, Capacitors, Diodes	1-2FIT
Low power BJTs, FETs	3-5FIT
Low complex analog ICs	5-10FIT
Switching regulators	10-20FIT
Power BJTs, FETs	60FIT
Mixed signal CMOS ASICs (50-500E6 transistors)	20-120FIT
MCUs	150FIT

Important note: These are "Base Failure Rates". E.g. static RAMs are affected by "Soft Errors" which add significant failure rate to these figures when not covered by ECC or parity.

Safety mechanism, diagnostic coverage, FMEDA

- **SM:** safety mechanism
  - A technical solution which typically prevent faults to become a single point failure
  - Controls AND/OR mitigates faults
- **DC**: diagnostic coverage (effectiveness of SM)
  - A coefficient ranging from interval 0-100%
  - Techniques and according DC values are listed in ISO26262-5
- **FMEDA:** failure modes, effects and diagnostic analysis
  - Typically a table listing components of the design
  - Failure modes of each and FM distribution
  - How are FMs covered by SMs
  - **Output:** calculated HW metrics

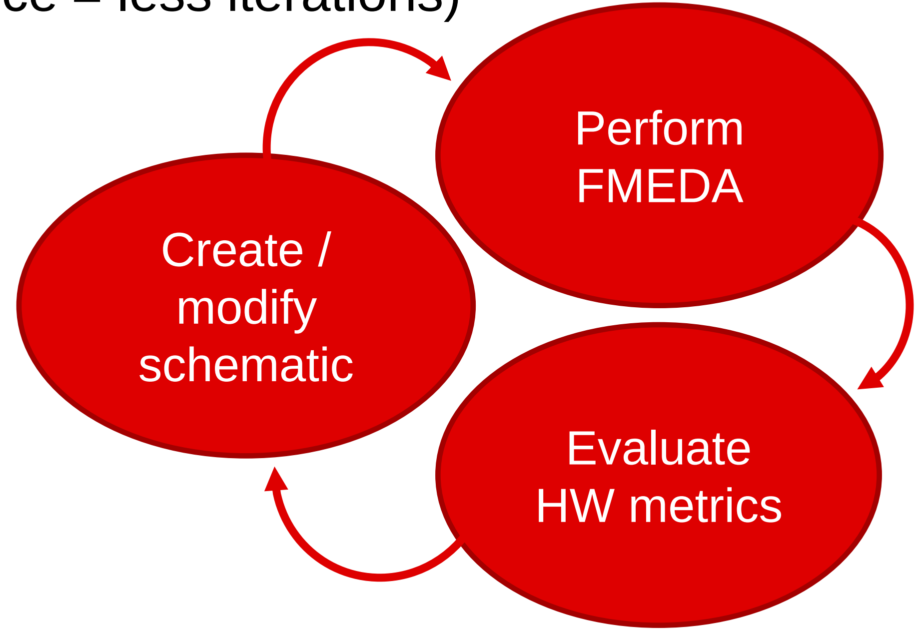
Hardware metrics

- Quantifies the effectiveness of the safety architecture
- Summary of **all** components relevant for a **safety goal**
- Calculations in the FMEDA table
- Three key metrics
  - Probability metric for random hardware failures (PMHF) – absolute value
  - Single point fault metric (SPFM) – ratio
  - Latent fault metric (LFM) – ratio

	ASIL B	ASIL C	ASIL D
PMHF	$<10^{-7}\,h^{-1}$ (100 FIT)	$<10^{-7}\,h^{-1}$ (100 FIT)	$<10^{-8}\,h^{-1}$ (10 FIT)
SPFM	>= 90%	>= 97%	>= 99%
LFM	>= 60%	>= 80%	>= 90%

FS hardware development simplified

- HW development philosophy according to ISO26262 is not different from good engineering practice
- Iterative process (experience = less iterations)



Example n=0

Zeroth iteration: Definition of Safety goal and setting the FS requirement

Safety goal:
Prevent overheating of the system (ASIL C)

Derived FS requirement:
Activate a cooling fan when the temperature rises above threshold

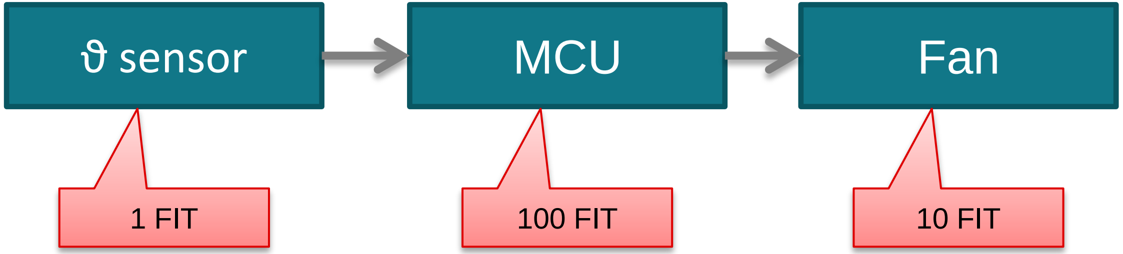
Example n=1

ASIL=N.A.

Single-Point Fault Metric=1-(56/111)=49.5%

Latent Fault Metric=irrelevant

PMHF=56FIT



	FIT	FMD	violates SG?	RF	MPF?	SM? (MPF)	DC-MPF-L	MPF-L
ϑ sensor	1	100%	Y	1				
MCU	100	50%	Y	50				
		50%	N					
Fan	10	50%	Y	5				
		50%	N					
Total	**111**			**56**				

Acronyms:

FIT = Failure In Time

SM = Safety Mechanism

FMD = Failure Mode Distribution

SG = Safety Goal

RF = Residual Faults (in FIT)

MPF? = Can cause Multiple Point Failures?

SM?(MPF) = Safety Mechanism with regard to MPF

DC-MPF-L = Diagnostic Coverage related to Latent MPF

MPF-L = Latent MPF

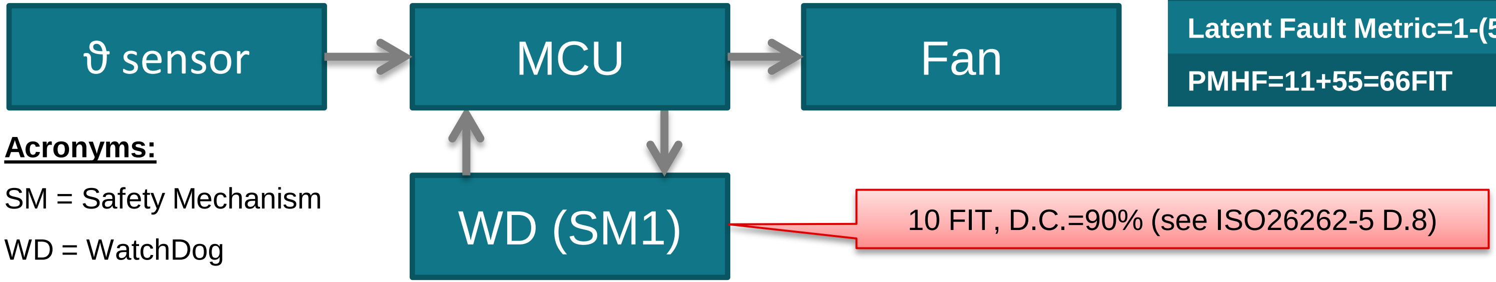
Example n=2

ASIL=N.A.

Single-Point Fault Metric=1-(11/121)=90.9%

Latent Fault Metric=1-(55/(121-11))=50%

PMHF=11+55=66FIT



Acronyms:

SM = Safety Mechanism

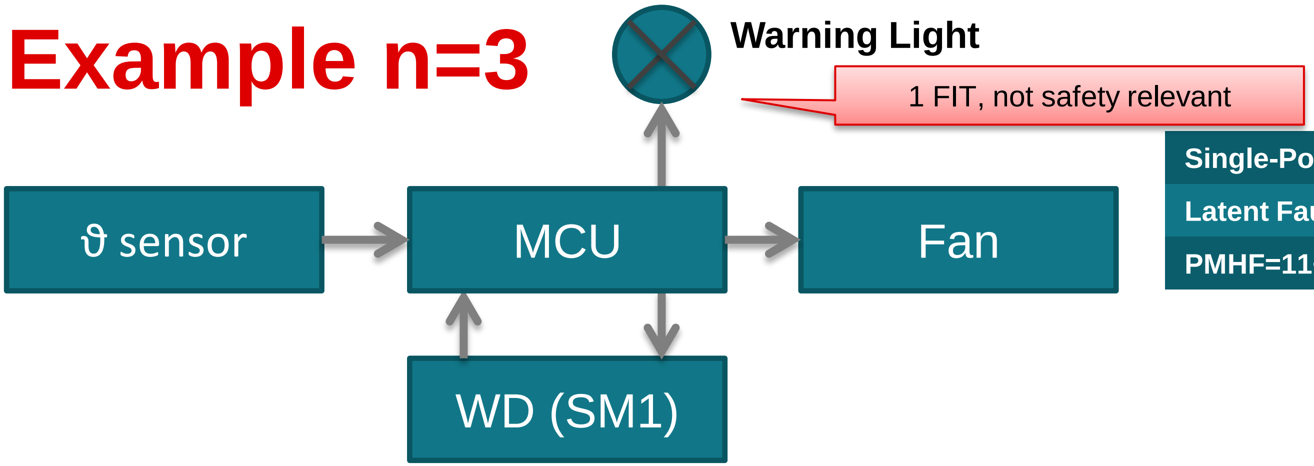
WD = WatchDog

	FIT	FMD	violates SG?	SM? (SPF)	DC-SPF	RF	MPF?	SM? (MPF)	DC-MPF-L	MPF-L
ϑ sensor	1	100%	Y	N		1				
MCU	100	50%	Y	SM1	90%	5		N	0%	45
		50%	N							
Fan	10	50%	Y	N		5				
		50%	N							
WD	10	100%	N				Y	N	0%	10
Total	**121**					**11**				**55**

Acronyms: SPF = Single Point Failures , SM?(SPF) = Safety Mechanism with regard to SPF, DC-SPF = Diagnostic coverage with regard to SPF

Example n=3

ASIL=B



Single-Point Fault Metric=1-(11/121)=90.9%

Latent Fault Metric=1-(10/(121-11))=90.1%

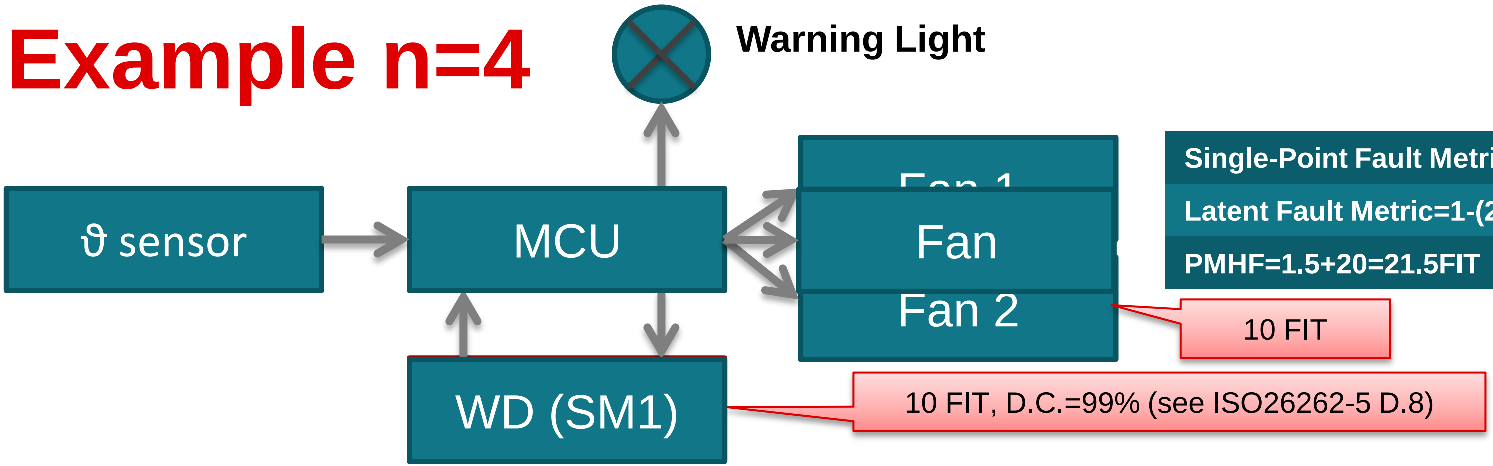
PMHF=11+10=21FIT

	FIT	Safety related?	FMD	violates SG?	SM? (SPF)	DC-SPF	RF	MPF?	SM? (MPF)	DC-MPF-L	MPF-L
ϑ sensor	1	Y	100%	Y	N		1				
MCU	100	Y	50%	Y	SM1	90%	5		N	100%	0
			50%	N							
Fan	10	Y	50%	Y	N		5				
			50%	N							
WD	10	Y	100%	N				Y	N	0%	10
Warn. Light	1	N	100%	N				N			
Total	**121**						**11**				**10**

Texas Instruments

Example n=4

ASIL=C



Single-Point Fault Metric=1-(1.5/131)=98.8%

Latent Fault Metric=1-(20/(131-1.5))=84.5%

PMHF=1.5+20=21.5FIT

	FIT	Safety related?	FMD	violates SG?	SM? (SPF)	DC-SPF	RF	MPF?	SM? (MPF)	DC-MPF-L	MPF-L
ϑ sensor	1	Y	100%	Y	N		1				
MCU	100	Y	50%	Y	SM1	99%	0.5		N	100%	0
			50%	N							
Fan 1	10	Y	50%	N	N			Y	N	0%	5
			50%	N							
Fan 2	10	Y	50%	N	N			Y	N	0%	5
			50%	N							
WD	10	Y	100%	N				Y	N	0%	10
Warn. Light	1	N	100%	N				N			
Total	**131**						**1.5**				**20**

Hardware element classes

ISO 26262-8:2018

Class I: Basic

- Few, if any sub-parts
- Failure modes easily identified
- No internal safety mechanism

Evaluation:

- no evaluation necessary

Class I: Basic

- Resistor, diode, relay, FET
- Op Amp, level shifter, logic gate, SVS
- single channel DCDC or LDOs
- Simple CAN or LIN TRX

How to address

- Typically no additional information besides the FIT rate necessary

Original slide credit: Ulrich Bertl

Hardware element classes

ISO 26262-8:2018

Class II: Intermediate

- Few operating modes
- Composed of sub parts
- Might have diagnostic function
- Operation and failure modes can be observed and tested for hardware qualification.
- Failure modes can be identified e.g. from datasheets or manuals

Evaluation:

- evaluation by analysis and testing

Class II: Intermediate

- ADCs, DACs, (digital) temp sensors (e.g. LM71), current sensors (e.g. DRV425, INA231)
- DCDC converter with power good
- TRX, general purpose SBC & higher function transceivers e.g. integrated CAN + LDO
- Multichannel and /or multifunction SVS

How to address

- Typically FIT rate and failure mode distribution
- pin FMEA

Original slide credit: Ulrich Bertl

Hardware element classes

ISO 26262-8:2018

Class III: Complex

- Many sub parts
- High complexity, many operating modes
- Failure modes identified with detailed knowledge only
- Internal safety mechanism relevant for safety concept

Evaluation:

- Should be developed in compliance with ISO26262
- Evaluation by analysis and testing
- Additional measures and arguments are required

Class III: Complex

Microprocessor, video accelerators, SOC (system on a chip), ECU, ECM

Multichannel PMICs (e.g. TPS65381, TPS65310, …)

- Motor driver (e.g. DRV3245)

- Higher function SBC (e.g. TCAN4550)

How to address

- FIT rate and failure mode distribution + pin FMEA
- Usually requires the part developed according to ISO26262

Original slide credit: Ulrich Bertl

FS components in TI's portfolio (SafeTI™ replacement)

http://www.ti.com/technologies/functional-safety/overview.html

TEXAS INSTRUMENTS

		Functional safety-capable The simplest product category of analog products that can be evaluated for use in a functionally safe system	Functional safety quality-managed Moderately complex products such as an MCU	Functional safety-compliant The most complex products such as MCUs, microprocessors and complex analog signal-chain products
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA*	✓	Included in FMEDA	Included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)*			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate**			✓

** May only be available for analog power and signal chain products. ** Available for select products.*

Backup

Quiz

What **system** ASIL level can be achieved with

A. Automotive rated logic gate e.g. SN74LV86A-Q1?

-> **ASIL D**. Logic gate is a low complex component and all failure modes are known and documented.

B. Functional safety quality-managed CAN-FD transceiver TCAN4550-Q1?

-> **ASIL D**. The documentation available from TI includes FMEDA and failure mode distribution analysis. The system integrator can easily evaluate the HW metrics as well as develop eventually safety mechanisms to mitigate the failures.

C. Functional safety compliant automotive gate driver unit DRV3245Q-Q1?

-> **ASIL D**. On top the documentation listed in previous case TI provides with a third-party certification report. Development process tailored for FS ICs and as well certified by a third-party.

Why & how do automotive and industrial systems differ?

	Automotive systems	Industrial systems
System characteristic	• Customizable • Configurable • Modular • Low cost	• One-purpose • Highly specific • Higher cost
Test for latent fault	~8h max drive cycle	24/7 continuous
Supply chain	Hierarchical • OEM • multiple Tier 1's, 2's	Flat One general supplier
Complete systems delivered	Very high volume	Lower volume

Why & how do automotive and industrial systems differ?

	Automotive systems	Industrial systems
Development process	Cost driven, Time-to-market	Reliability, availability –driven
Safety assessment	Hierarchical – per element (even down to IC level)	Flat – one large safety assessment after commissioning the complete system
Components used	State of the art	Well proven in use
Architecture	Typically single-channel with emphasise on diagnostics (1oo1D)	Typically redundant symmetric architecture (1oo2D)