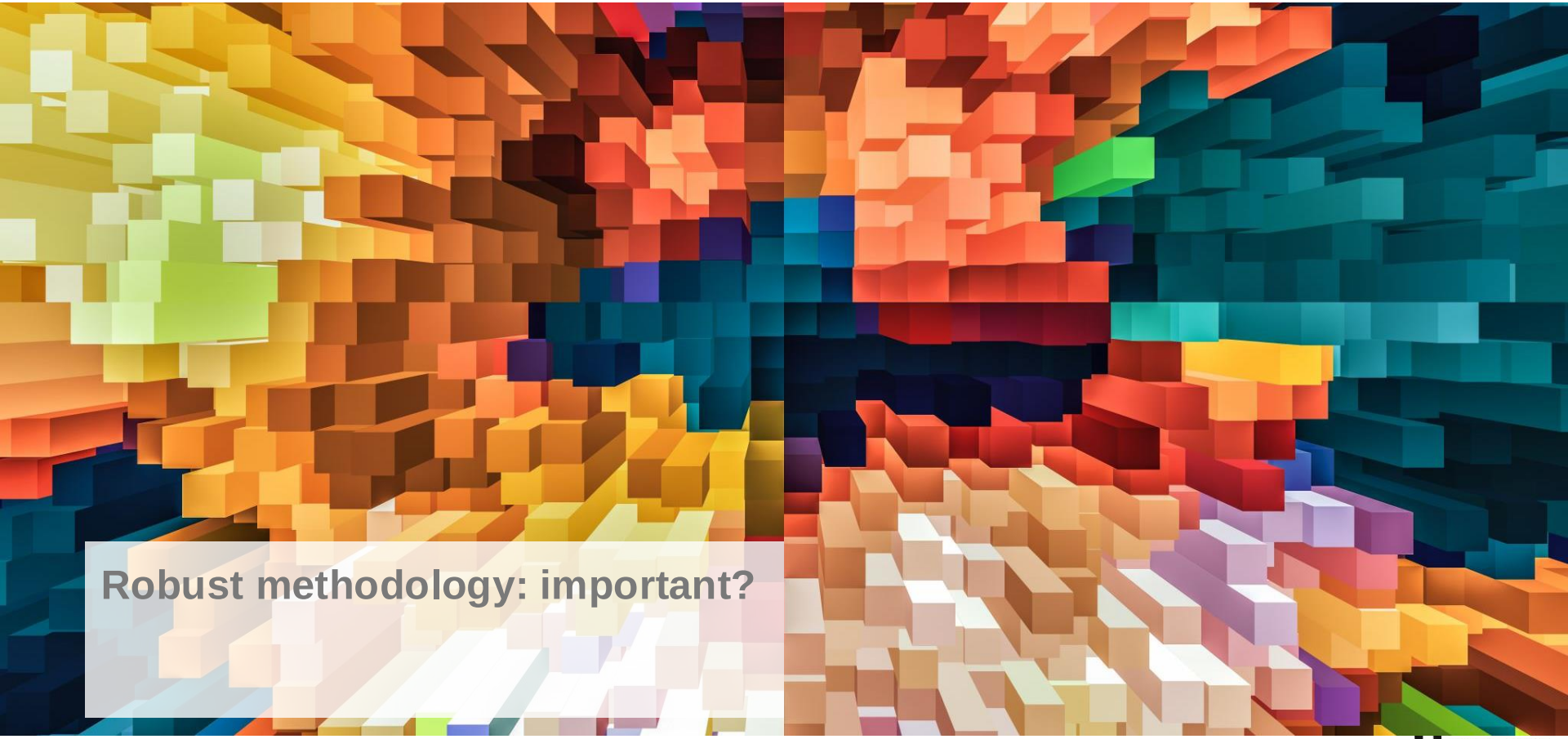
MASTER OF SCIENCE IN ENGINEERING

MA_EmbReal

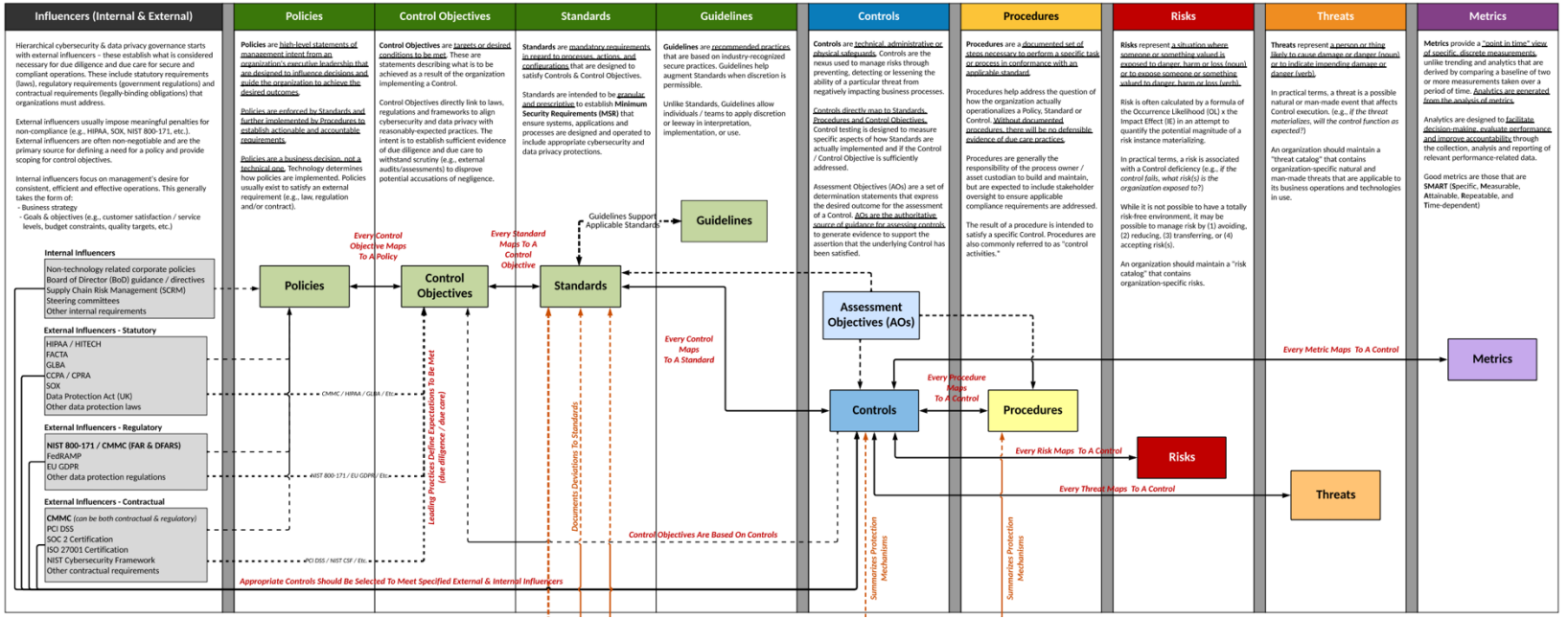
Robust Development Methodologies I

Version: 1.3

Serge Ayer – Luca Haab | 04.03.2025 | Cours MSE


Robust methodology: important?

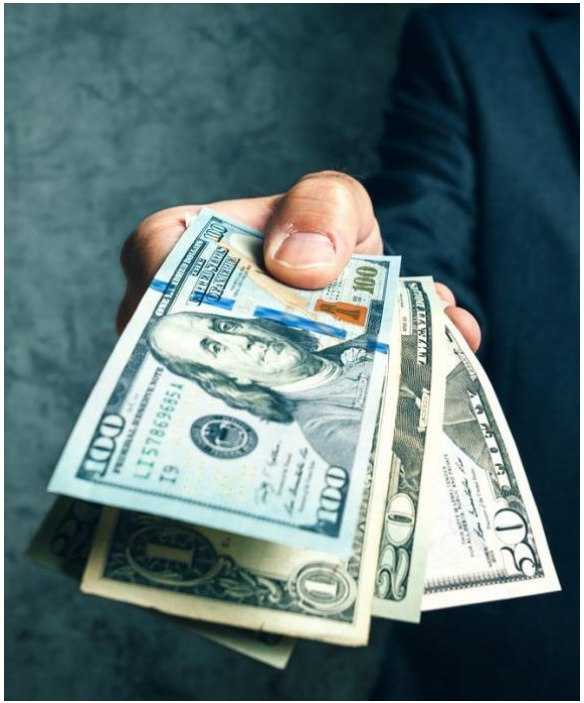
Policies vs Standards vs Guidelines vs Procedures



Source: https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf

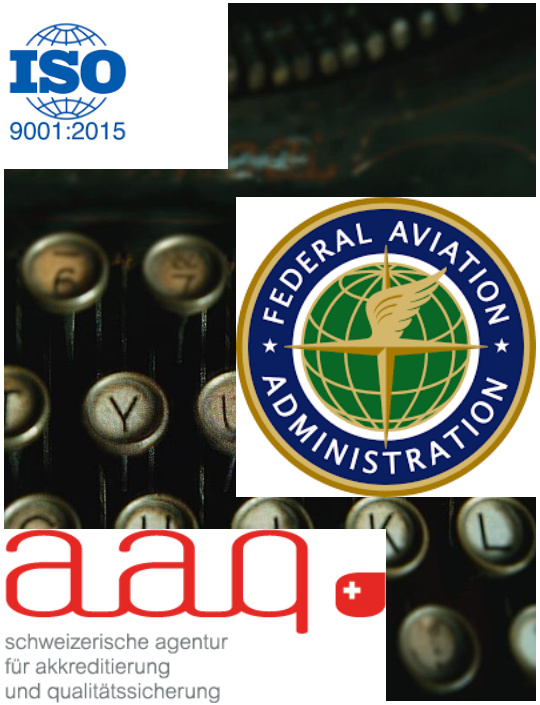
Standardization

- Companies want standardization as it allows them to:
  I. **maximize** the business benefits;
  II. **institutionalize** the best practices in standards;
  III. **be compliant** with contract obligations, national laws regulations & directives.



Standardization: Main Goals

Standardization != Certification



- Standard = formulae that describes the best way of doing something
- Certification = provision by an independent body of written assurance (a certificate) that specific requirements are met

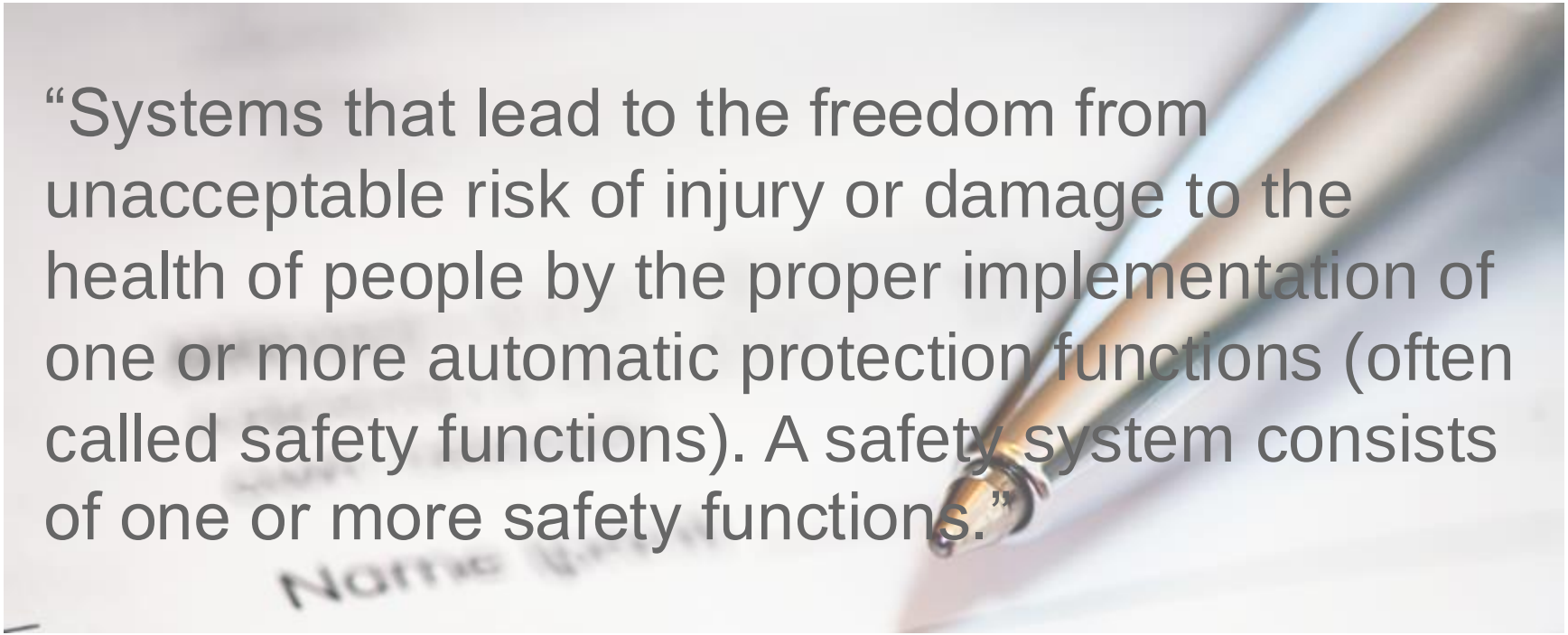
Sum-Up: Certification only?

CYTRICS: an example

- Ensures fulfillment of necessary quality
- Allow preferred access to market
- Defines obligations and gives guarantees

Safety: Goals

Safety System: Definition

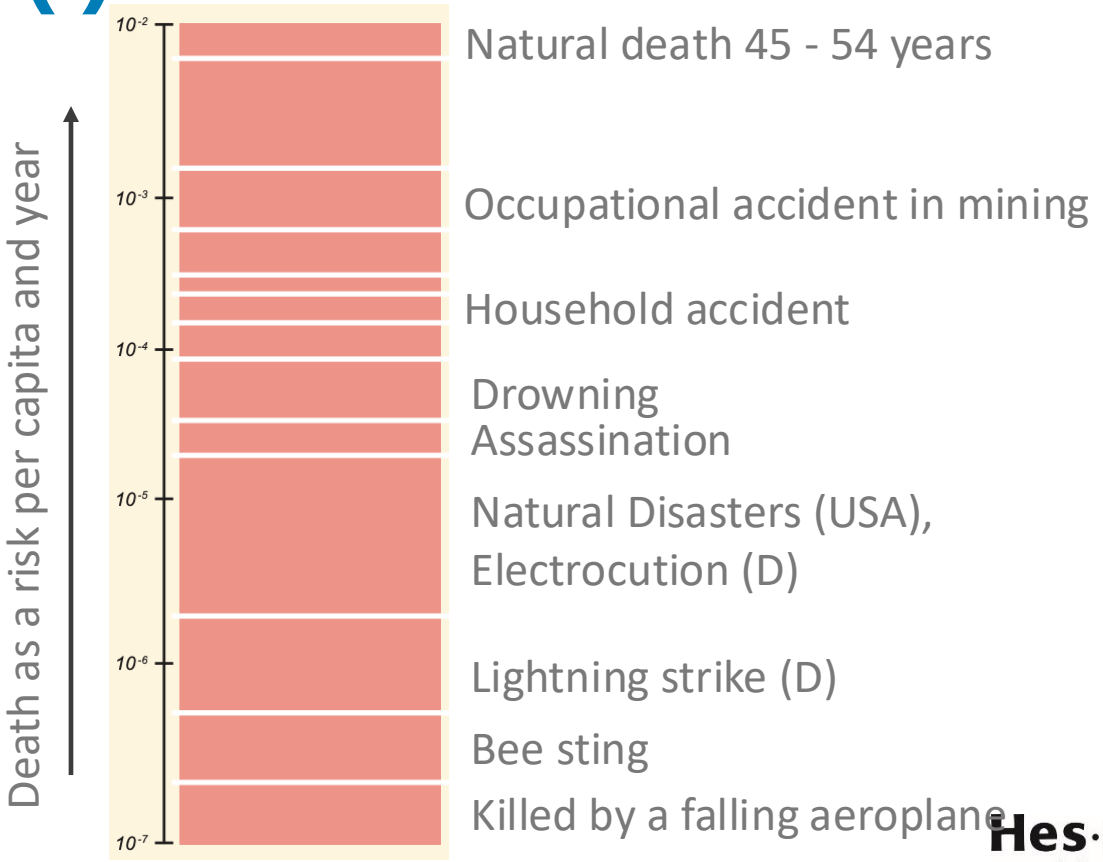


"Systems that lead to the freedom from unacceptable risk of injury or damage to the health of people by the proper implementation of one or more automatic protection functions (often called safety functions). A safety system consists of one or more safety functions."

Source: https://www.tuvsud.com/en-us/services/functional-safety/about

Safety: Standards

Safety: Risks (I)



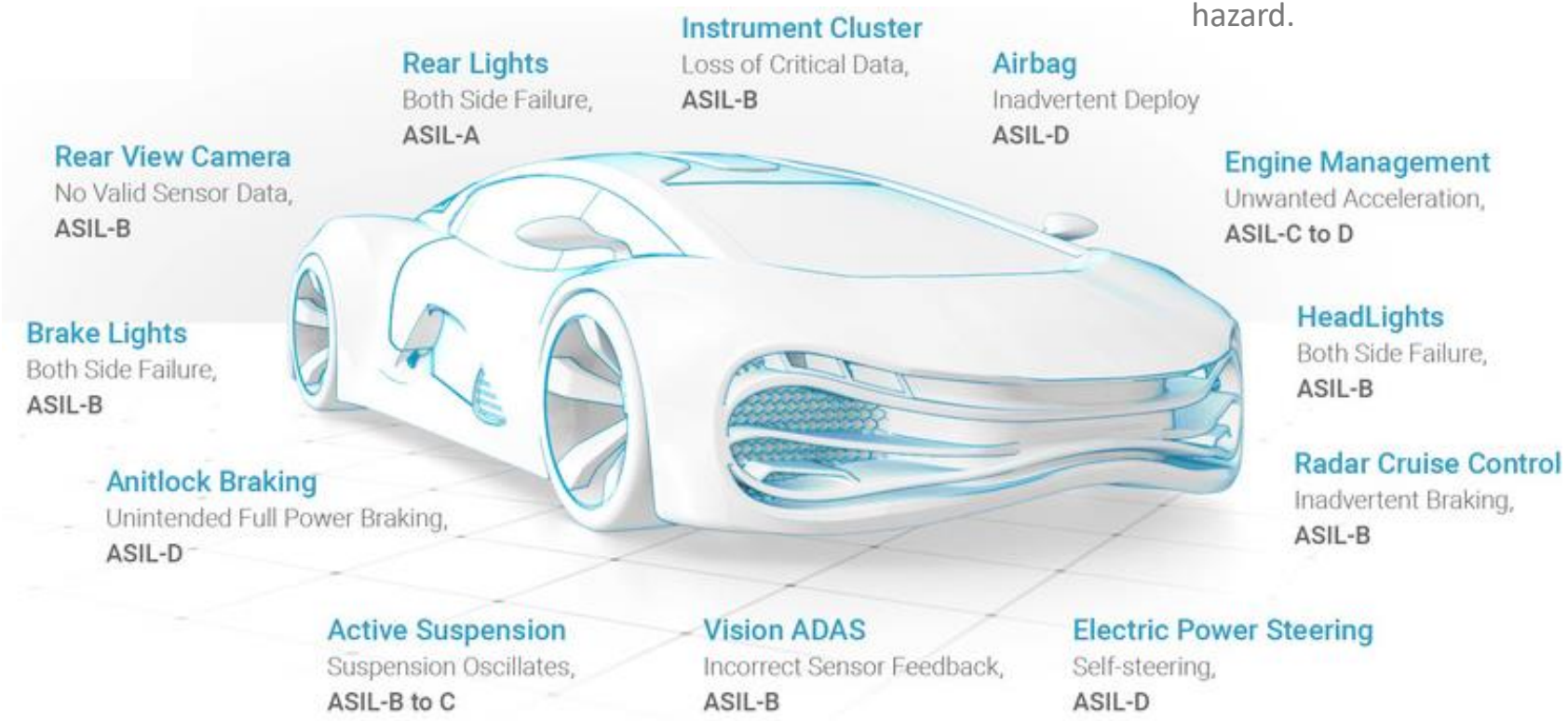
Safety: Risks (II)

SIL	Low Demand Mode: Average Probability of Failure on Demand	High Demand or Continuous Mode: Probability of Dangerous Failure per Hour
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$ (1 dangerous failure in 1140 years)
4	10^{-5} to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

IEC61508 SIL: Safety Integrity Level

Safety: Risk is Varied

ISO 26262: ASIL A represents the lowest and ASIL D represents the highest degree of automotive hazard.



Source: https://www.synopsys.com/automotive/what-is-asil.html

Safety: ASIL

For each electronic component engineers need to consider:

- Severity
- Exposure
- Controllability

Severity has four classes:

- From “no injuries” (S0) to “life-threatening/fatal injuries” (S3).

Exposure has five classes:

- From “incredibly unlikely” (E0) to the “highly probable” (E4).

Controllability has four classes:

- From “controllable in general” (C0) to “uncontrollable” (C3)

Safety: ASIL for ABS

Malfunction — ABS system failure

↓

Hazard Analysis — What unintended situations (hazards) could happen? → Loss of stability on split-μ surface

↓

Risk Analysis
- How likely is the hazard to happen? (Exposure) → Oil spill, gravel, water potholes...
- How harmful is the hazard? (Severity) → Car may spin out of control and crash
- How controllable is the system if the hazard occur? (Controllability) → Dashboard, driver

↓

ASIL Determination — What level of safety (risk reduction) does the system need?
- How likely can the malfunction be? → **Failure Rate**
- How often does the system need to catch it and get to a safe situation? → **Effectiveness of failure detection (SPFM, LFM)**

Low — ASIL (Automotive Safety Integrity Level) — High

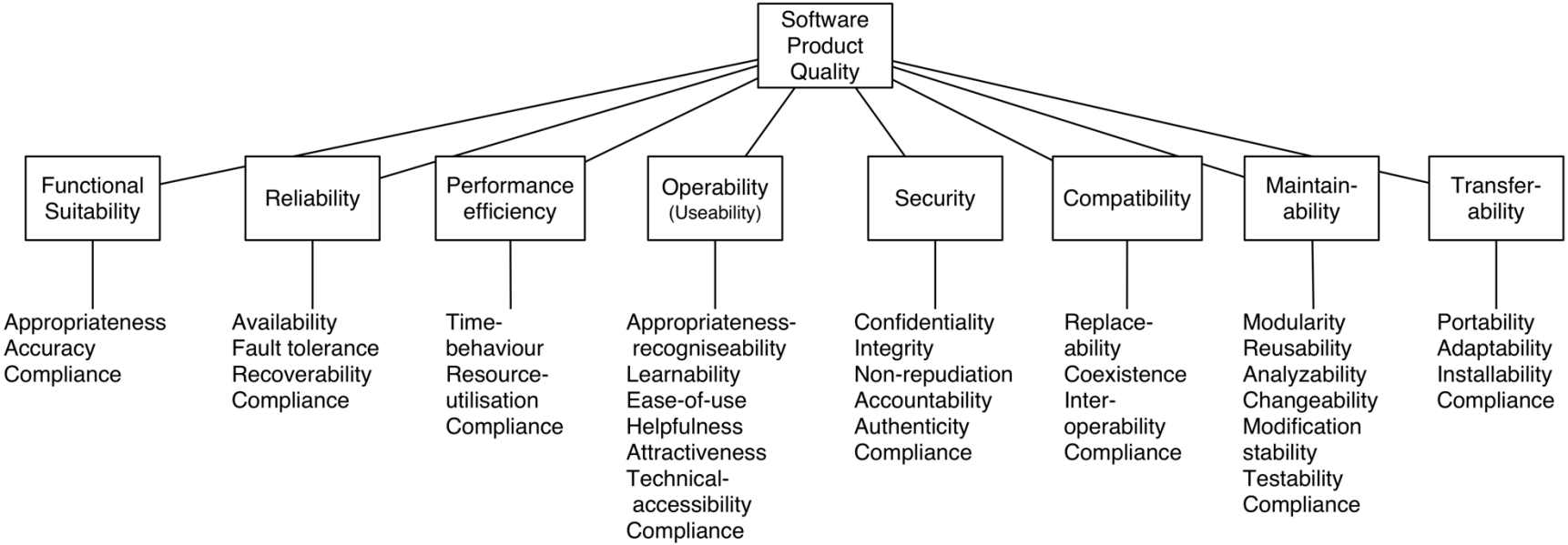
A B C D

Reduce Failure Rate, Increase Effectiveness of Failure Detection (SPFM, LFM)

Source: https://www.embitel.com/wp-content/uploads/ABS.jpg

Source: https://www.aptiv.com/images/default-source/feature-stories/asil-diagram-v01.png?sfvrsn=d47cbf3e_4

SW Quality: ISO 25010



Source: https://nocomplexity.com/wp-content/uploads/2016/08/ISO-25010-QualityTree.png

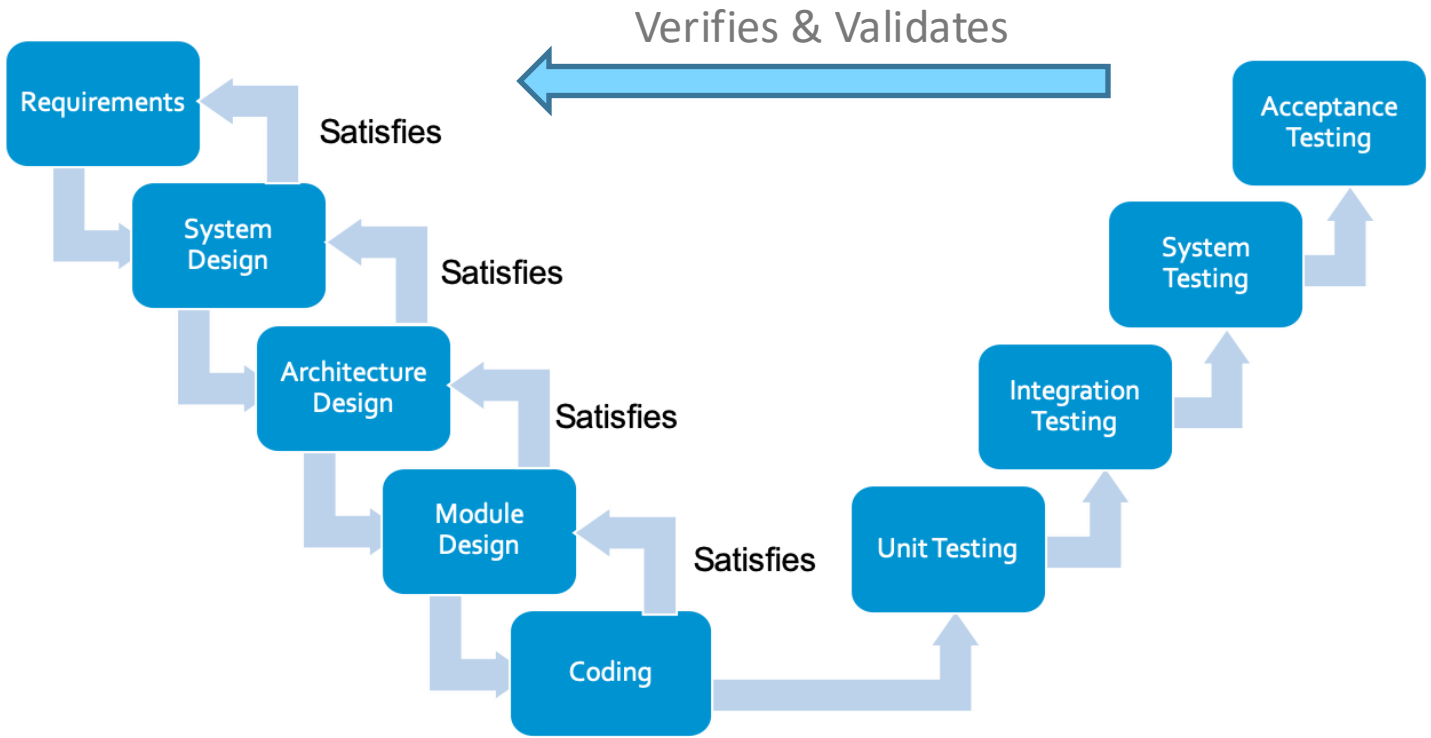
Standards & Guidelines: what now?

Break any of these rules sooner than say anything outright barbarous.

- George Orwell (Politics & English language)

Example: https://google.github.io/styleguide/cppguide.html

Crucial: Traceability



Source: https://www.parasoft.com/wp-content/uploads/2020/06/V_Diagram_Traceability_Figure1.png

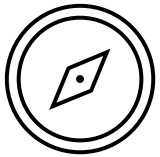
MISRA

MISRA guidelines are a) part of standards or b) a way to fulfil standards mandatory guidelines

- MISRA started in the early 1990s as UK government's "SafeIT " whose target was to develop guidelines for road vehicle electronic systems.
- MISRA provides world-leading best practice guidelines for the safe and secure application
- Has since transformed into a consortium regrouping all major industry secure and safe embedded players

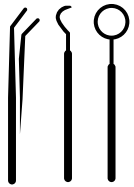
MISRA Introduction (I)

Staff training



Style guide enforcement

Metrics measurements



Tool management

Run-time behaviour

MISRA Introduction (II)

Achieving compliance with MISRA Coding Guidelines

Section	Guidance
2.3	Staff have been trained in the use of the programming language within embedded system
7.1	Staff have been trained in the use of The Guidelines
2.4	These is a process for enforcing a style guide
2.5	These is a process for enforcing code metrics
2.6.3	There is a process for dealing with deficiencies in the compiler's implementation
2.6.3	There is a process for dealing with deficiencies in the analysis tool's implementation
2.6.4	A choice has been made between possible versions of the programming language
2.6.4	The translator has been configured to accept the correct version of the programming language
2.6.4	The translator has been configured to generate an appropriate level of diagnostic information
2.6.4	The translator has been configured appropriately for the target machine
2.6.4	The translator's optimization level has been configured appropriately
2.6.5	The analysis tools have been configured to accept the correct version of the programming language
2.6.5	The analysis process can deal with any language extensions that have been used
2.6.5	The analysis tools have been configured for the implementation, for example to be aware of the sizes of the integer types
2.6.6	There is a process for ensuring that the program has sufficient resources, such as processing time and stack space
2.6.6	There is a process for demonstrating and recording the absence of run-time errors, for example in module designs
3.3	There is a GEP showing how compliance with each guideline is to be checked
3.4	There is a process for investigating and resolving any diagnostic messages produced by the translator
3.4	There is a process for investigating and resolving any diagnostic messages produced by the analysis tools
3.5	There is a process to manage undecidability issues
4	There is a deviation process for recording and approving deviations
5.1	There is a GRP showing how each guideline is to be enforced
7.3	There is a GCS showing the level of compliance which is being claimed

Process and tools checklist

GEP: guideline enforcement plan
GRP: guideline recategorization plan
GCS: guideline compliance summary

Source: https://www.misra.org.uk/app/uploads/2021/06/MISRA-Compliance-2020.pdf

MISRA Introduction (III)

Guideline Enforcement Plan (GEP)

Guideline	Compilers		Analysis tools		Manual review
	'A'	'B'	'A'	'B'	
Dir 1.1					Procedure x
Dir 2.1	no errors	no errors			
...					
Rule 4.1			message 38		
Rule 4.2				warning 97	
Rule 5.1	warning 347				
...					
Rule 12.1				message 79	
Rule 12.2			message 432		Procedure y
Rule 12.3			message 103		
Rule 12.4				message 27	

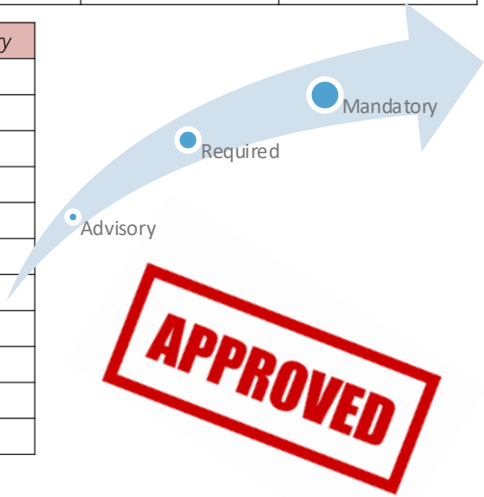
Guideline Compliance Summary (GCS)

Guideline	*MISRA Category*	Compliance
Dir 1.1	Required	Compliant
Dir 2.1	Required	Deviations
...		
Rule 4.1	Required	Deviations
Rule 4.2	Advisory	Disapplied
Rule 5.1	Required	Compliant

Guideline Recategorization Plan (GRP)

MISRA category	*Revised category*			
	Mandatory	Required	Advisory	Disapplied
Mandatory	Permitted			
Required	Permitted	Permitted		
Advisory	Permitted	Permitted	Permitted	Permitted

Guideline	*MISRA category*	*Revised category*
Dir 1.1	Required	Mandatory
Dir 2.1	Required	Required
...		
Rule 4.1	Required	Required
Rule 4.2	Advisory	Disapplied
Rule 5.1	Required	Mandatory
...		
Rule 12.1	Advisory	Mandatory
Rule 12.2	Required	Required
Rule 12.3	Advisory	Advisory
Rule 12.4	Advisory	Required



Source: https://www.misra.org.uk/app/uploads/2021/06/MISRA-Compliance-2020.pdf

MISRA Introduction (IV)

- Decidability
  - A rule is decidable if it is always possible to answer with an unequivocal “Yes” or “No”
  - A rule is undecidable if an analysis tool cannot guarantee a “Yes” or a “No” in every situation

```
extern void f ( uint16_t * p );

uint16_t g ( void )
{
  uint16_t x;    /* x is not given a value                                  */

  f ( &x );      /* f might modify the object pointed to by its parameter */

  return x;      /* x may or may not be unset                               */
}
```

How can you assess “The value of an object with automatic storage duration shall not be read before it has been set” for g?
(without analysis, which may be impossible)

Source: https://www.misra.org.uk/app/uploads/2021/06/MISRA-Compliance-2020.pdf

MISRA C:2012: simple example

- Directive 4.4 states “Sections of code should not be ‘commented out’”

```
void D_4_4 ( void )
{
   int32_t a;

   /* a = 3;   Non-compliant  */
   a = 1;
   // a = 3;   Non-compliant

   use_int32 ( a );
}
```

Source: https://gitlab.com/MISRA/MISRA-C/MISRA-C-2012/Example-Suite/-/blob/master/D_04_04.c

MISRA C:2012: D || R

- **Directive**
  Is a guideline for which it is not possible to provide the full description for a compliance check

  ➞ tools deliver widely different results

- **Rule**
  Is a guideline for which a complete description of the requirement has been provided

MISRA: want to know more

Check out https://youtu.be/Mrf7rIJxgI8
(MISRA C in the ISO 26262 Context, by Andrew Banks, Chairman - MISRA C Working Group)