ISO 26262
Main Experiences Introducing the Standard in Organizations this Year

John Favaro, Giovanni Sartori

Auto&Rail RAMS & Q.A. Business Unit INTECS, Pisa, Italy

A Year in ISO 26262

- ISO 26262 came of age in 2011
- Many organizations have had to confront the new standard on two levels:
  - **Conceptual**: new approach, terminology, …
  - **Practical**: new processes, techniques, …
- We have spent much time this year introducing ISO 26262 into organizations on both levels

Conceptual

A Year in ISO 26262 Teaching

American ~~Dream~~ Nightmare

- April 2011 – Detroit
- Heterogeneous group from many organizations
- Several senior level engineers
  - Some contrast to European course populations
  - Good: great contributions
  - Bad: sometimes preconceptions formed over many years
- High degree of preoccupation with costs of implementing the standard
- Perplexity about relationship to AUTOSAR

Tangled Terminology

- Tangled terminology
  - FMEA experts – but what does “severity” mean?
  - Often serious terminological confusion

Potential Failure Modes and Effects Analysis

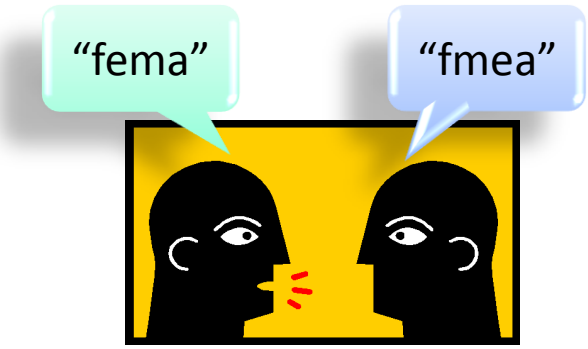
System _____ FMEA Revision _____

Subsystem _____ FMEA Prepared By _____

Part Number _____ FMEA Date _____

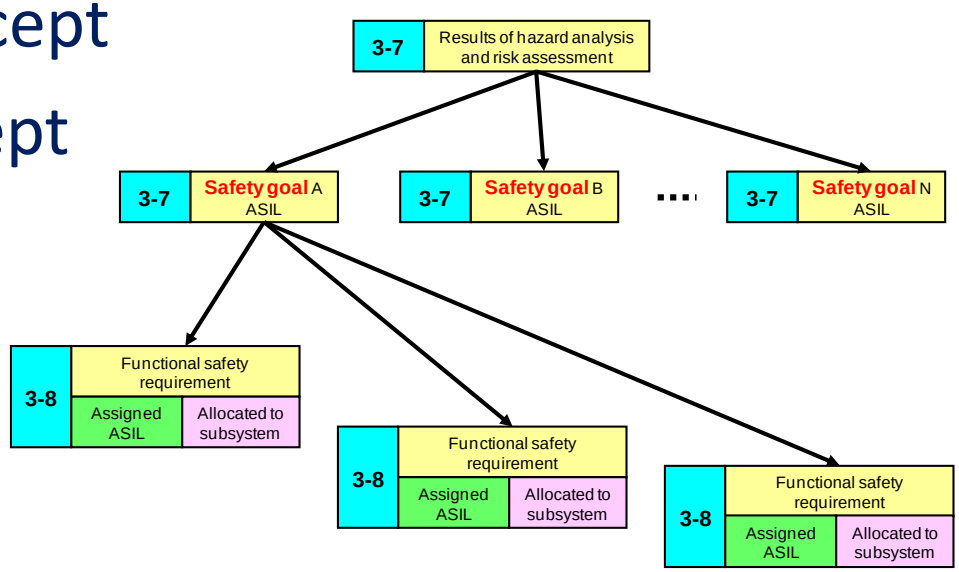
Designer _____ FMEA Revision Date _____

Item/ Function	Potential Failure Modes	Failure Mode Effects	S E V	Potential Failure Causes	P F	Current Controls	D E T	R P N	Actions Req'd	Owner/ Target Date	Actions Taken	S E V 2	P F 2	D E T 2	R P N 2



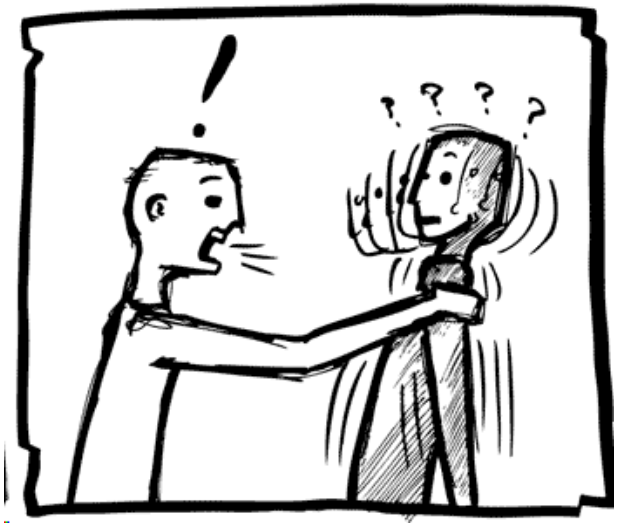
Straight Down

- Requirements development exercise
  - Create a hierarchy of requirements
- Straight to the solution
- No concept of layers of abstraction
  - Functional safety concept
  - Technical safety concept
  - System
  - Hardware, software



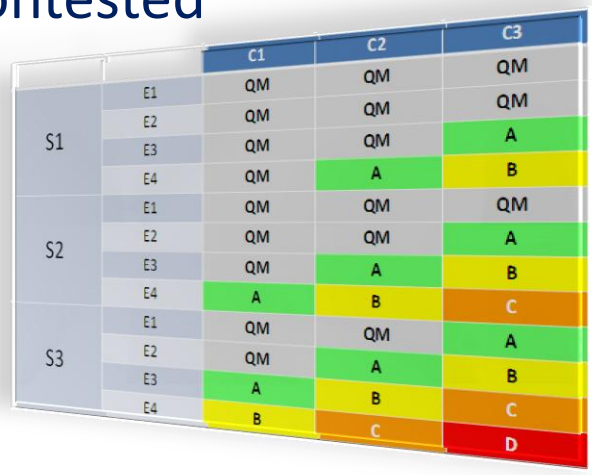
Convincing the others

- Sometimes participants could only be convinced by *other* participants
  - The value of process
  - System level decision-making authority
  - What is the *really* hard part? From B to C or from nothing to something?
  - No reverse engineering of safety
- The value of safety as a group experience



Fatal Hazard Analysis Exercise

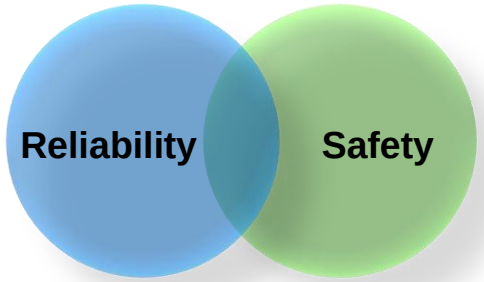
- Concept Phase – Hazard Analysis and Risk Assessment
- Exercise: separate into teams and do a hazard analysis and risk assessment
  - Agreement among experts on expected results
- (Nearly) universal failure
  - Extreme controversy
  - Those who were “right” were heavily contested
  - “Shock and awe” the principal reaction



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Safety Culture

- "Before 26262," people often think they already have a safety culture – but they don't
  - You don't arrive at a safety culture by intuition
- Reliability and safety?
  - Reliability is about the *probability* of failure
  - Safety is about the *consequences* of failure
  - There are different questions to answer



intecs
the Brainware company

Practical

A Year in ISO 26262 Projects

First Steps into ISO 26262 (1)

Project independent

- Company Functional Safety policy definition
- Definition of interaction with the Quality department
- Company guidelines
- Tools selection, templates, dB
- Collection of Lessons-Learned
- Training for involved personnel
- Lifecycle definition
- Roles and responsibilities

First Steps into ISO 26262 (2)

Project dependent

- Safety plan: creation and maintenance
- Evidence: document every activity performed
- Confirmation measures: independence level definition
- Safety case: creation and maintenance
- V&V activities for Functional Safety
- Definition of post-SOP (*Start Of Production*) rules for Functional Safety

Hazard Analysis: some pitfalls

- Analyze item *without* safety mechanisms
- Bad/poor/unclear definition of item's functions
- Mixing hazards and hazardous events
- Hazard not evaluated at vehicle level

H.A.: slicing too much …

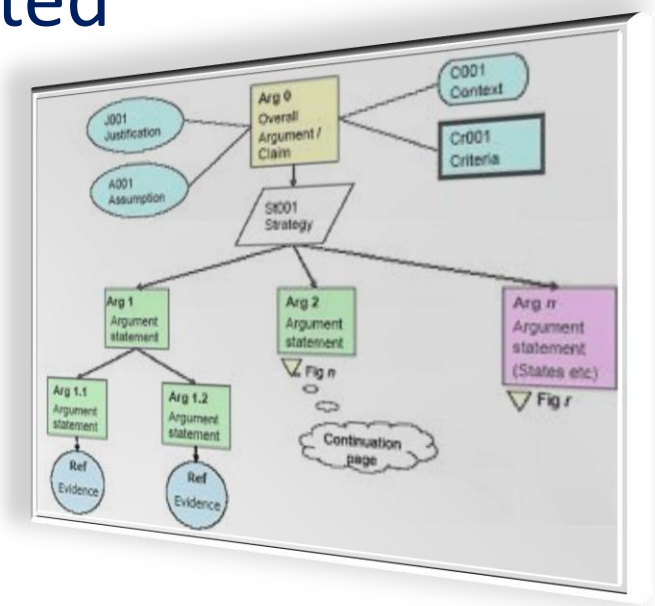
- Problem affecting real Hazard Analysis
- A scenario is split into multiple sub-cases in order to reduce the E/C/S index value
- A lower ASIL is obtained in this way

But this is the **wrong** way!!

- Scenarios have to be realistic for getting a clear understanding of hazards

Safety case: sooner or later?

- The safety case should be done early in the project, not as it is ending
- I.e. start it at completion of the concept phase
- Consider S.C. as a support in evaluating if the proposed solution can be supported by sufficient evidence through appropriate arguments



ISO 26262 Certification: yes or no? 1/2

- ISO 26262 does not mention the term certification
- ISO 26262 requires only an assessment

But, is that all?

- The manufacturing company can ask for a certification of product/process
- Some organizations state that a F.S. assessment internally done may not be sufficient in case of a trial

ISO 26262 Certification: yes or no? 2/2

- Currently, we know that the trend is for an accredited body certification of:
  - ***Tools (SW mainly)***
  - ***Semiconductors (IP, µP, ASICs …)***
  - ***Safety processes***

And what about items?

- Up to now, the combination of some audits and functional safety assessment seems to be enough

Cover it, please!

- A common misunderstanding in SW Unit tests
- The goal: testing the SW units against the SW unit design specification for verifying compliance
- Coverage is a sort of “effect”, it’s not the goal!
- Avoid designing test cases from the actual source code
- The glitch: 100% covered source code **does not necessarily** mean 100% compliant software

Pret a porter or customized?

- Lifecycle tailoring is possible for modification
- Perform an impact analysis for identifying areas affected by modifications
- Changes in calibration or in configuration data are can affect the behavior of the item, so they are modifications!

- Update safety plan with the needed activities

Grazie!

john.favaro@intecs.it
giovanni.sartori@intecs.it