September, 2018

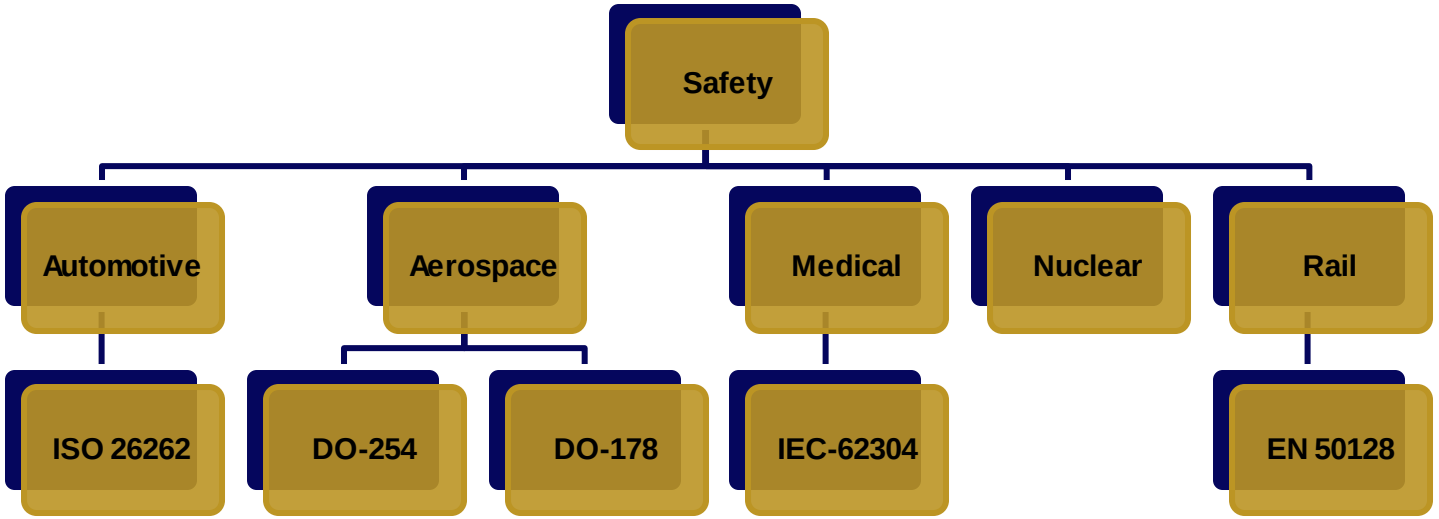
The Verification Challenges in Safety Compliance

Mike Bartley, T&VS

Test and Verification Solutions

Background

- **A number of companies are contemplating the automotive market**
  - but there are significant barriers to entry including ISO26262 compliance.
- **Other markets (e.g. drones, robotics) also have regulatory compliance barriers.**

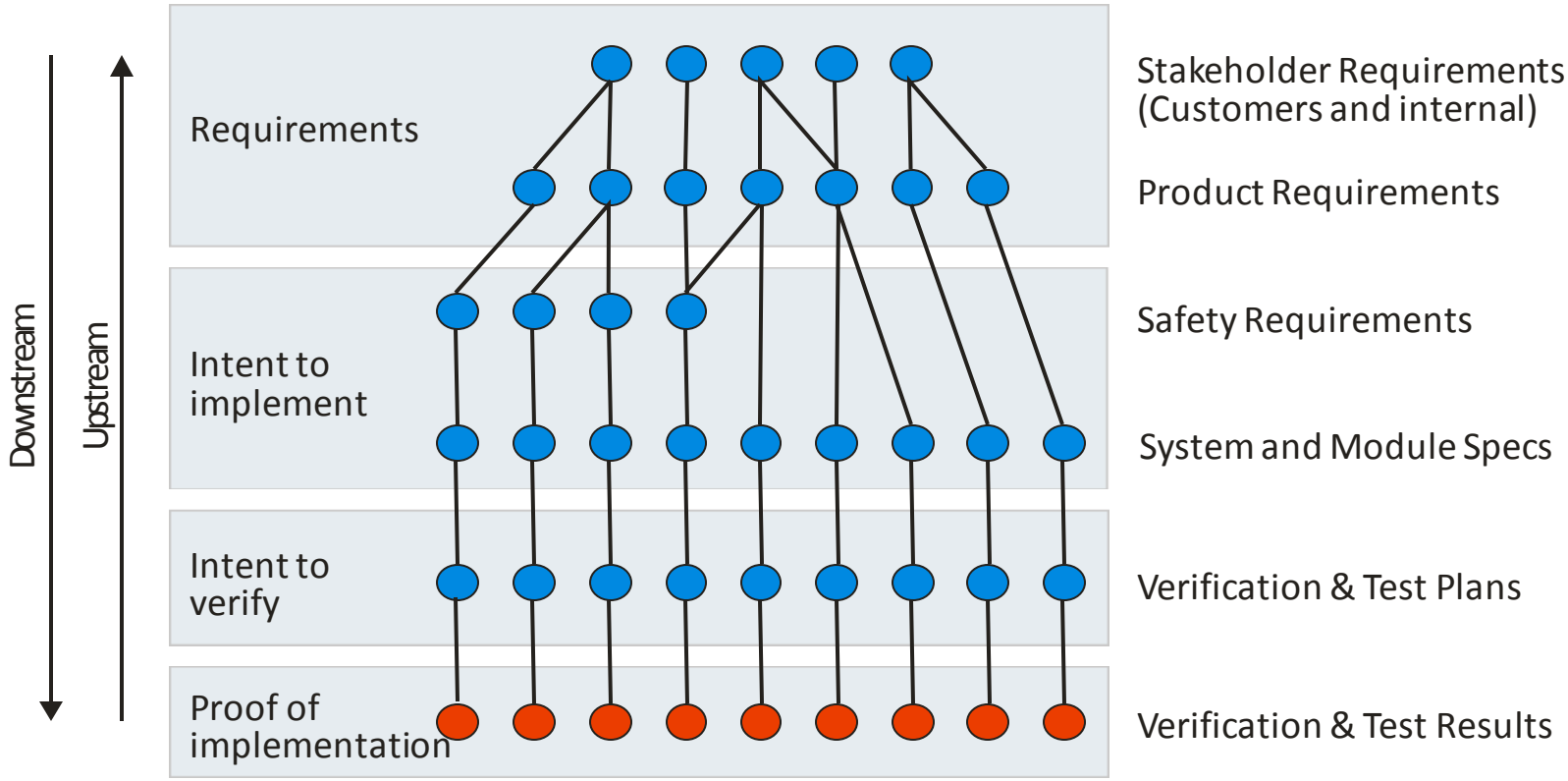


- **The 2 main safety verification challenges in demonstrating compliance to such safety regulations**
  - Requirements tracing
  - Fault analysis

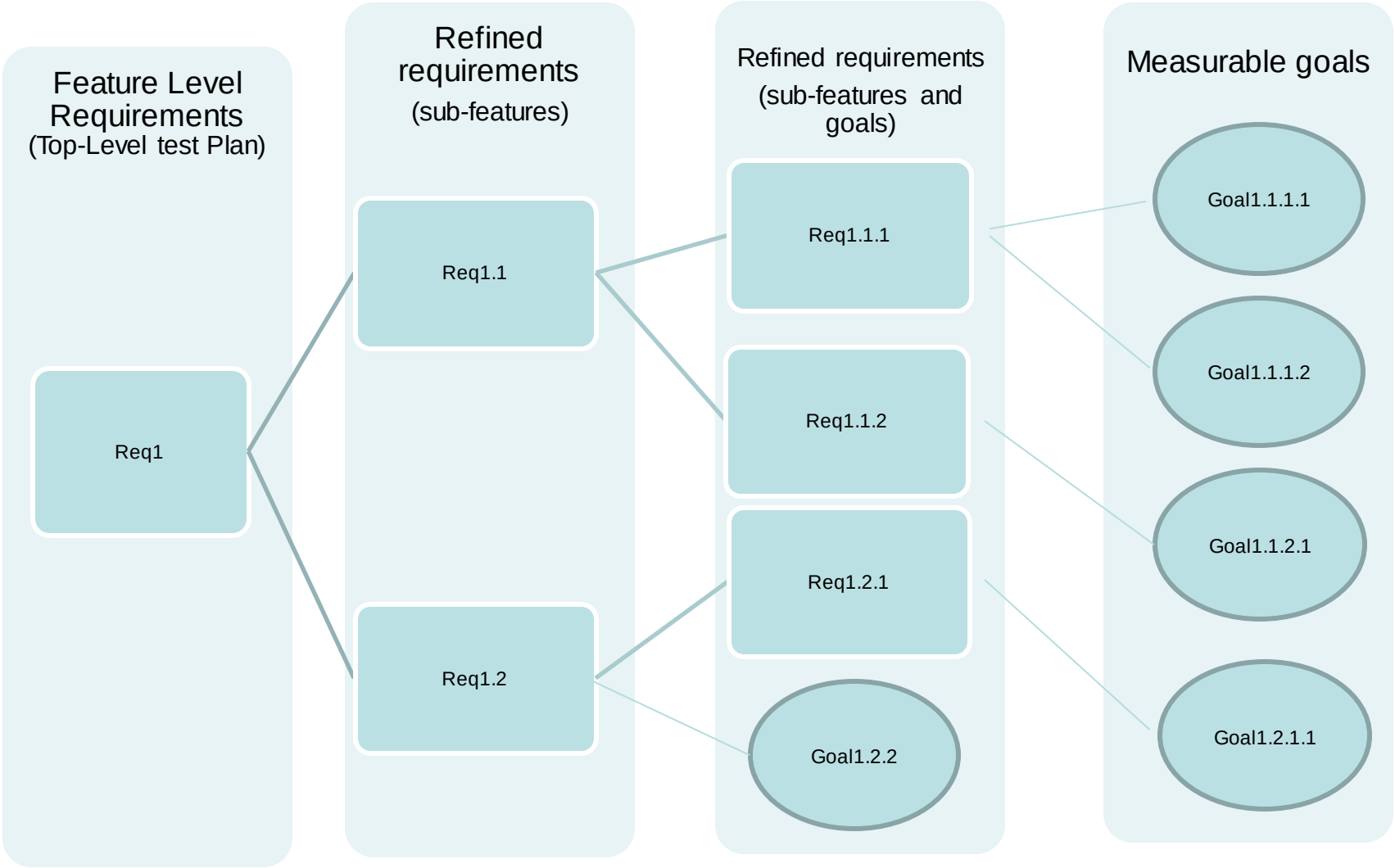
Requirements Management

ISO 26262 Stipulates

"The management of safety requirements includes managing requirements, obtaining agreement on the requirements, obtaining commitments from those implementing the requirements, and maintaining traceability."



REFINING THE REQUIREMENTS TO TEST DESCRIPTION LEVEL



Fault Analysis: How Systems Fail

- **Random failures**
  - Usually predictable
    - We know expected frequency of such failues
  - Can undertake preventative activities
- **Systematic failures**
  - We can't usually predict these – so we check
    - Is the system specified, designed and implemented correctly?
    - Did we follow a well-managed development process?
    - Did we generate all of the required development artefacts?
- **Systemic failures**
  - Shortcomings in culture or practices

- **We perform a Risk Analysis to determine our tolerance to failure**

ISO 26262 Risk Analysis

S = severity of injur(ies)
E = frequency/duration of exposure to hazard
C = controllability of hazardous event by driver or other traffic participant

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

ASIL:
Automotive Safety Integrity Level

ASIL A = lowest
ASIL D = highest

Higher ASIL
- More Rigorous Verification Process – e.g. higher levels of code coverage
- Higher levels of random fault detection

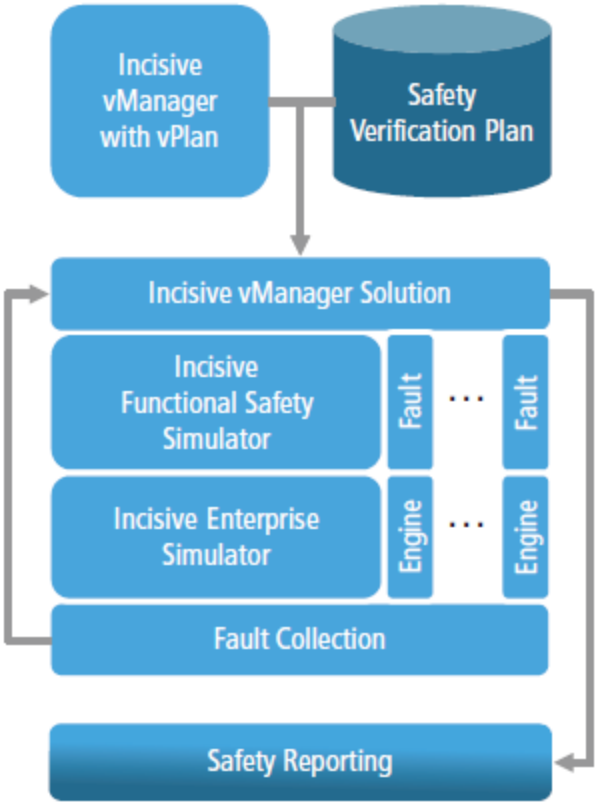
Protection from faults

- **Designing protection from faults**
  - Permanent faults
  - Transient faults
- **Must be able to detect certain %**
  - Exact % depends on ASIL
- **Design techniques**
  - ECC to detect and correct single bit faults
  - ECC to detect multi-bit faults
  - Lock step designs
  - Software runs regular “DfT” patterns

Fault Simulations

- **Identify fault model**
  - Permanent faults, transient faults, etc
- **Inject faults into design**
  - On RTL and Gate-level Netlists
- **Run regression suite**
  - Do we hit the fault
  - Does the design detect the fault
- **Objective**
  - Measure the % of faults detected

- **Also**
  - Verify lock step
  - Verify software can load and run DfT configurations



Cadence Flow

Partners for Safety Verification

- **Cadence**
  - Provides the tools you need
- **T&VS**
  - Provides the expertise and the services you need

September, 2018

THANK YOU

Test and Verification Solutions