# Tier1 perspective on ISO 26262 – Confirmation Measures

# How do we know we're doing enough to address safety?

Or.....

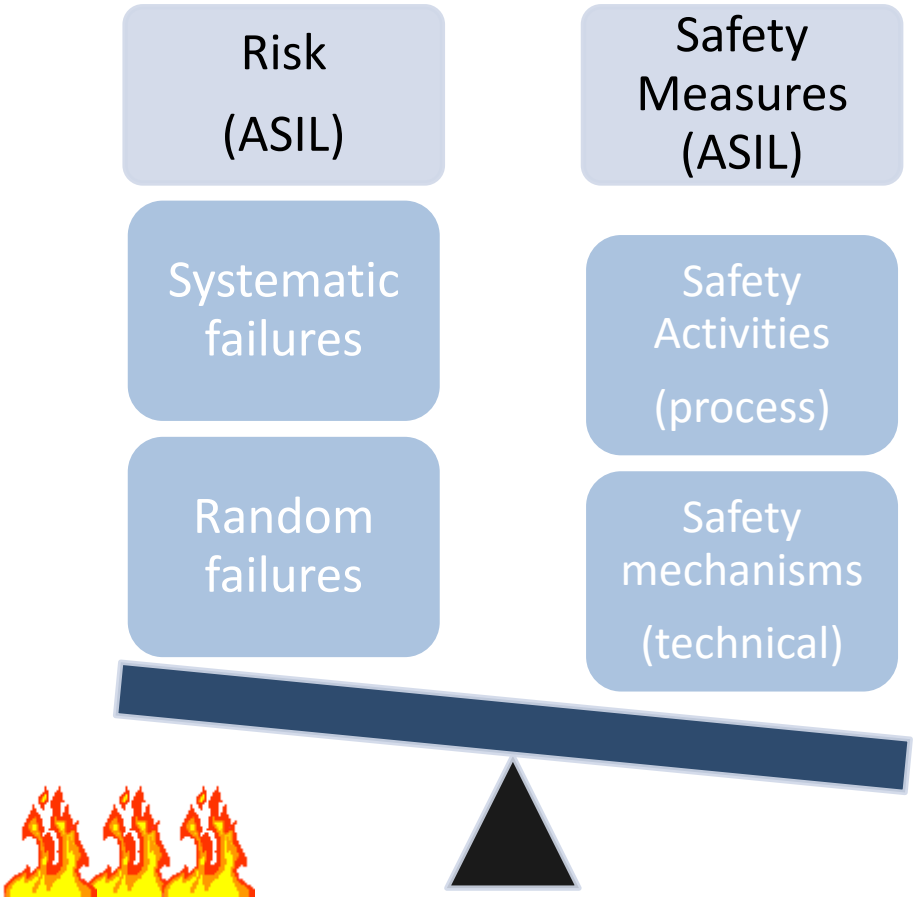
- How can we demonstrate we've done enough?

- A safety standard provides guidance as to what to do but not how to do it
- Whilst we aim to "confirm" we also wish to uncover any weaknesses ASAP prior to production.

- ISO 26262 provides "**Confirmation Measures**" to help address this

# ISO 26262 Recap

ASIL is the degree of  unacceptable risk due to malfunctioning behaviour of an “Item”
The safety measure inherits the ASIL to indicate the “level” of risk reduction.



Assessment, Audit and Confirmation Reviews

# OVERVIEW OF CONFIRMATION MEASURES

# Confirmation Measures

**Functional Safety Audit**

- What: Process implementation
- When: process enactment, completed prior to safety assessment

New

**Confirmation Reviews**

- What: specific lSO 26262 isted work products
- When: after associated safety activity, all completed before safety assessment

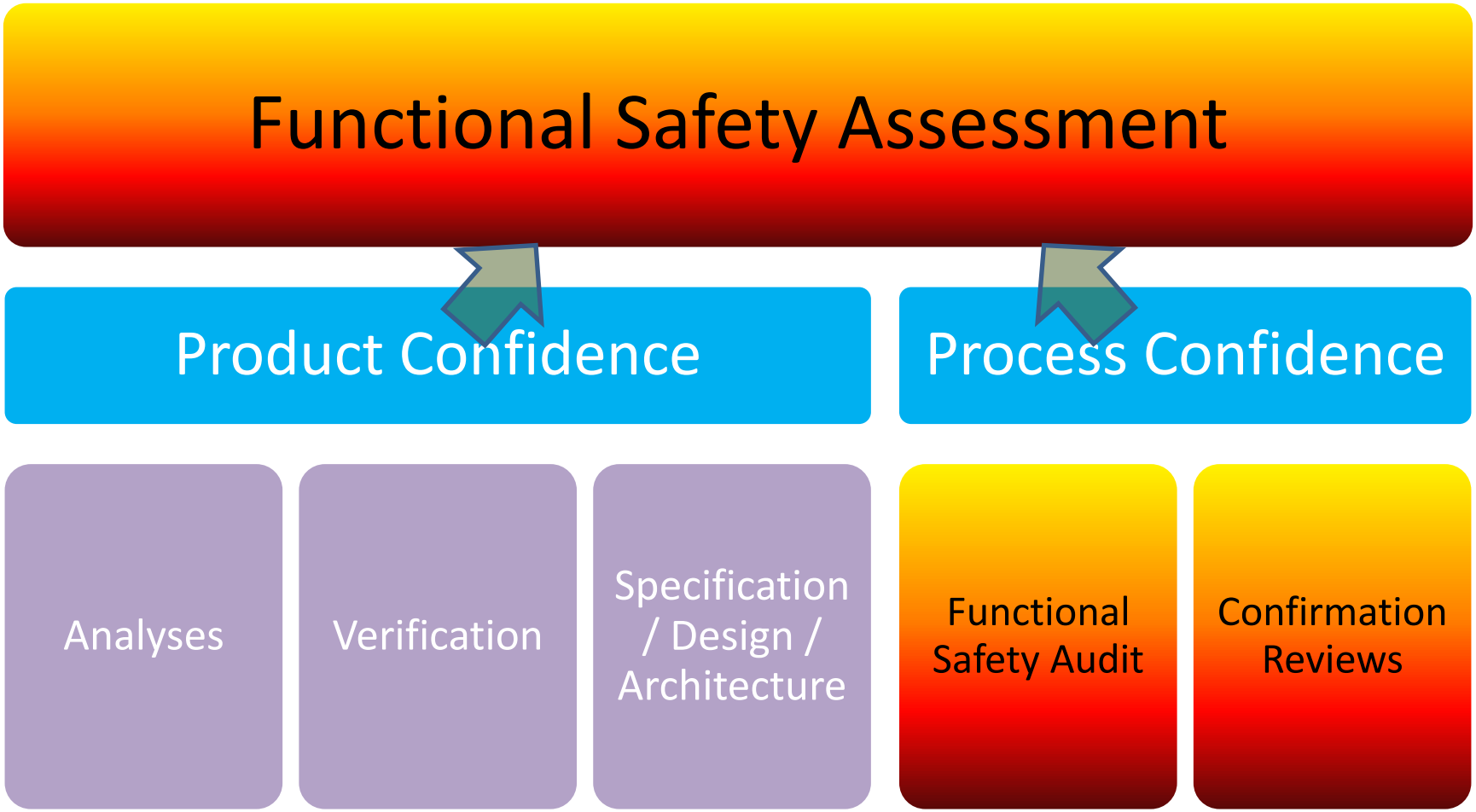
New

**Functional Safety Assessment**

- What: Safety Case - argument and evidence of safety of “Item”
- When: completed prior to release for production (single event or progressively)

Activities (requiring “Independence”) that are dependent on the maximum ASIL of the safety goals.

# Confirmation Measures in relation to development




**Good practice suggests confirmation measures phased to, and performed in lockstep with development – from concept to release for production.**

Confirmation Reviews vs Verification Reviews

# **CONFIRMATION** REVIEWS

# The “review” in “Confirmation Review”:

- **Review**:

Focus: work product
Objective: achievement of work product goal (wrt the purpose of the review)

Everything and anything e.g. tech, process, competency etc.

- **Verification**:

Focus : requirements (of the product).
Objective: complete and correct specification or implementation

Technical

- **Verification Review:**

Focus : “project requirements, or technical requirements”
Objective: development activity fulfils requirements

Technical. But what are “project requirements”?

- **Confirmation Review:**

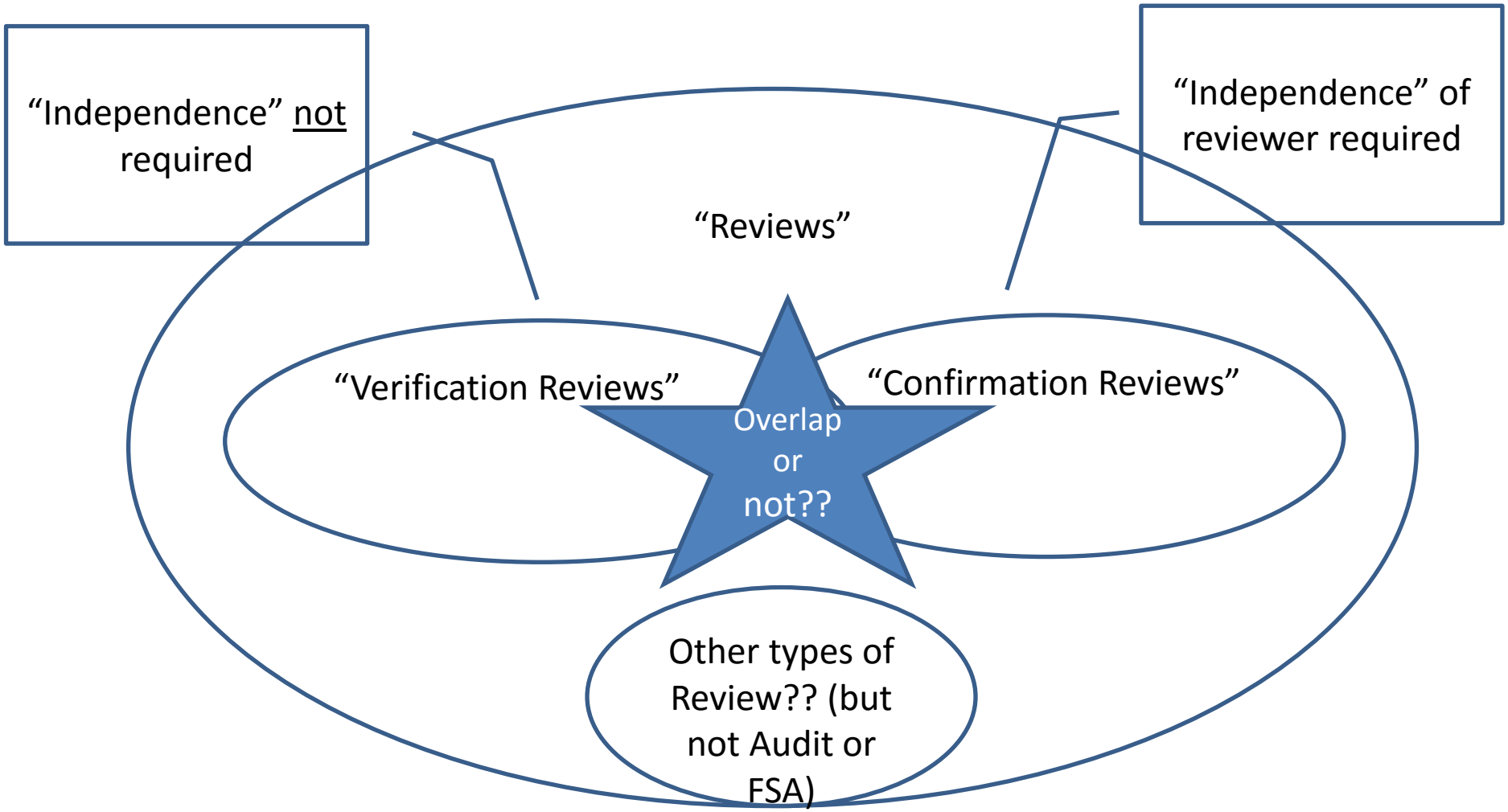
Focus: specific subset of ISO 26262 work products
Objective: “compliance” with the requirements of ISO 26262

Process (compliance). A “special” review, requirement for “Independence”

# Verification Review vs Confirmation Review

- Prior to ISO 26262, verification reviews typically covered process aspects.
- Verification Review
  - Product focus
- Confirmation Review
  - Process confidence
- Potentially some confusion or inefficiency??

# Can a Confirmation Review be a Verification Review? (or vice a versa)




Venn diagram

# Confirmation Reviews
# Proposals for ISO 26262 2nd Edition

- Scope of Confirmation Reviews to become assessment-like activity.
  - Judgement of the contribution to achievement of safety
  - Supporting the principle of phased, iterative assessments

# FUNCTIONAL SAFETY ASSESSMENT

# Can functional safety be achieved with a non-compliance?

- General consensus is that it may be so – depending on the non-compliance.
  - 100% compliance is questionable in any case
- Proposal for 2nd edition to make FSA objective based
  - Where each major clause has defined objective
  - Audit and Confirmation reviews still important input
  - Emphasis aimed at technical aspects

# Assessment Procedure and Competency

- Assessment requires a certain skill set and experience
  - From technical and procedural perspectives

- Technical: by an assessment “team” approach
- Procedural: via skill set akin to auditors, plus...
  - Guidance also available from UK’s ISA working group
    - Independent Safety Assurance http://www.theiet.org/factfiles/isa/
  - CASS
    - IEC 61508 - Conformity Assessment of Safety-related Systems

# Final Thoughts

- Efficient combination of verification and confirmation reviews
- Functional safety Assessment
  - Competency of Assessment/Assessor
    - Emphasise the technical to counter the tendency audit
    - Maintaining independence of assessments in balance with required technical expertise
  - The Safety Case – a “compilation of evidence” is not easy to assess without argument/claims
  - Similarly with out process / audit confidence  assessment may be impractical
- Confirmation Reviews
  - A focus on aspects contributing to achievement of safety
- All three confirmation measures to be performed in a timely manner to uncover any issues ASAP
- Confirmation Measures are intended to provide redundant checks on development activities and not to devolve the team of responsibilities

# Thanks for your time, any questions?


- *'Insanity: doing the same thing over and over again and expecting different results.'* Albert Einstein
- *'The prevention of hazards shall not be seen as following law, but merely as an act of human responsibility and economic reason.'* Werner von Siemens, 1880
- *"ISO 26262 = engage brain and keep it engaged" Roger Rivett*
- *"It's good that it's better, but it would have been better if it was good" anon*

Dave Higham – Functional Safety Senior Technologist