



*Welcome
to
GlobalCompliancePanel's
Live Webinar*

Residual Risk and Risk based Verification

Tuesday, August 09th, 2011

10:00 AM PDT | 01:00 PM EDT

By Markus Weber, System Safety, Inc.

Course Disclaimer

The information provided in this webinar is taken from sources and material which we believe to be reliable, and/or express the opinions of the writers and/or presenter. In such condensed and generalized form, the material certainly should not be considered a complete study or report on the subject matter, especially as to how it might relate to a specific company / user's application. Conclusions are based solely on available data, and the judgments and analysis of technical factors offered are not intended to replace the utilization of additional research and/or appropriate professional counsel in adapting material to a specific application.

© 2011 by System Safety, Inc. All rights reserved. Reproduction in whole or in part without written permission is prohibited.

Purpose

- Verification planning during the Risk Management Lifecycle
- Reduce verification resources and time
- Increase test quality and effectiveness
- Ensure safety and efficacy without compromising project time

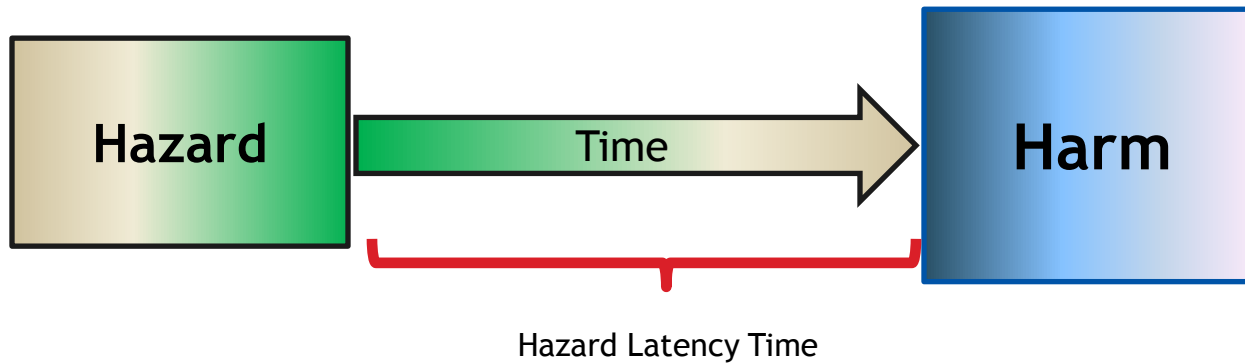
Risk Management

Process of:

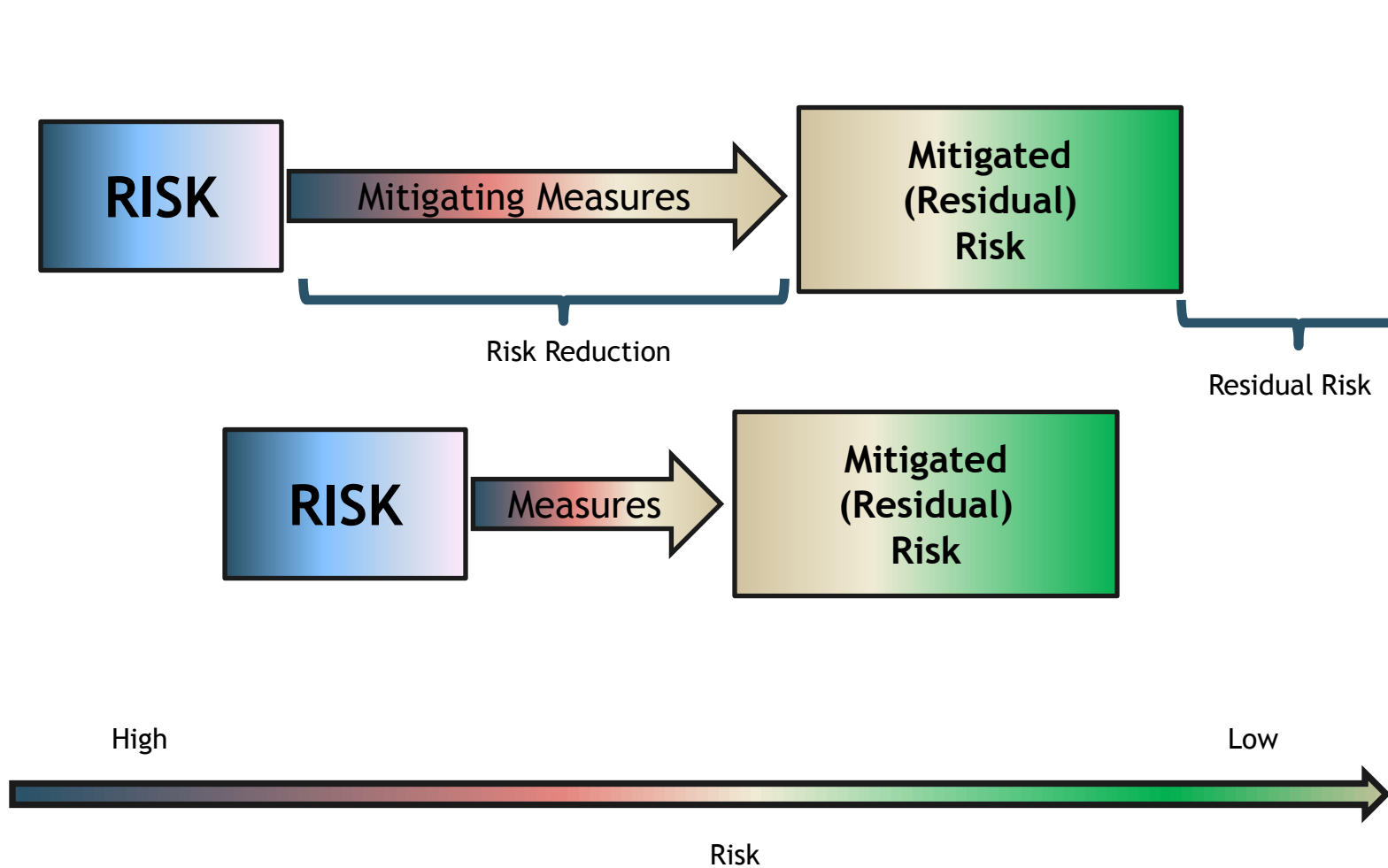
- identifying
- reducing
- managing
- and verifying

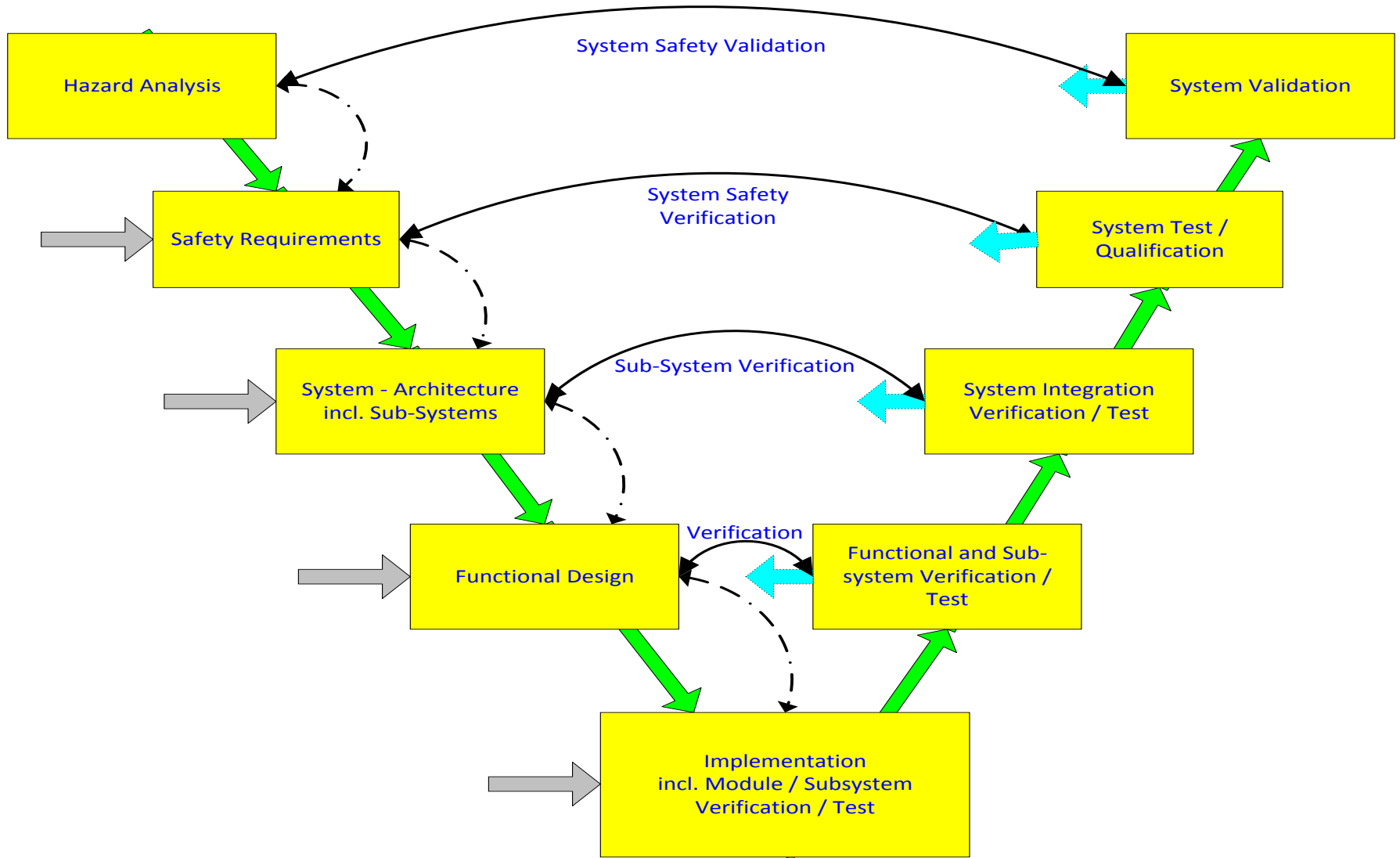
risk and risk reduction throughout the device development and deployment (the entire product life cycle).

Harm turns into Hazard



Residual Risk





Requirements

- Define the device functionality and documentation
 - Functional requirements
 - Efficacy requirements
 - Safety requirements
 - Documentation requirements
- Are often associated with subsystems
 - Hardware requirements
 - Software requirements
 - User interface requirements
 - Environmental requirements

How to define a Requirement?

- “Shall” signifies a mandatory requirement
- “Should” signifies an optional requirement

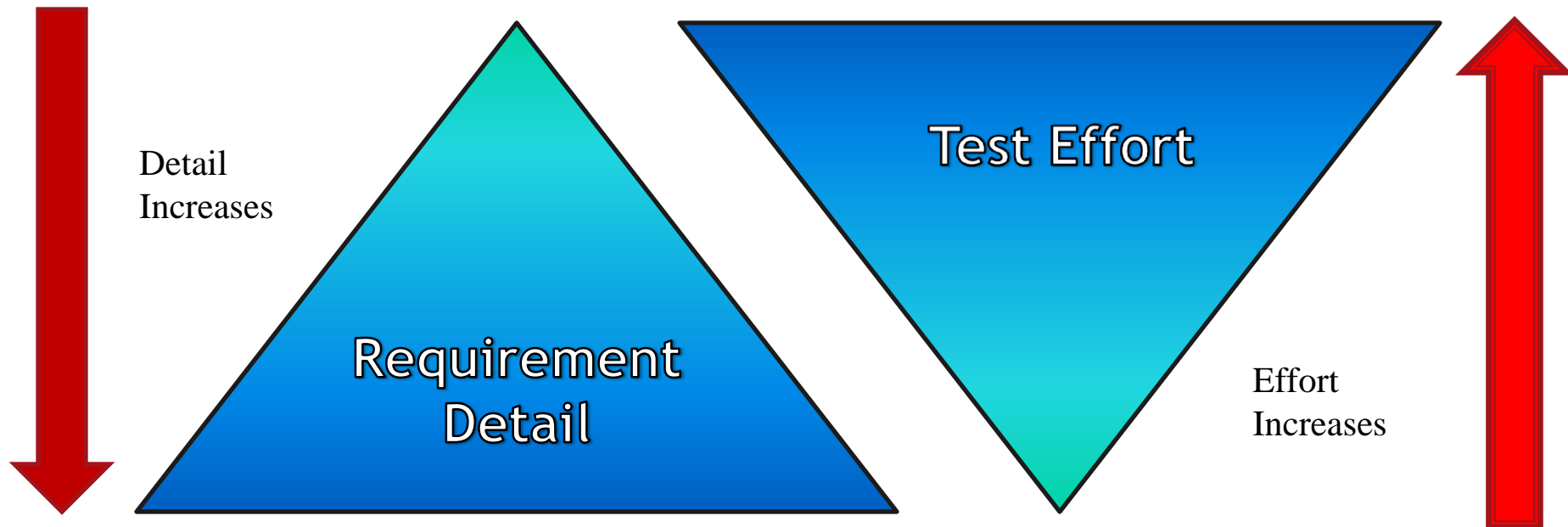
- Example:
 - The xyz shall weigh below 4 Kg.
 - The xyz should be easy to carry.

- “Shall” requirements need to be verified!

What is a Requirement ?

- Describe the system / module behavior:
 - Complete (all requirements)
 - Correct
 - Conflict free
 - Unambiguous
 - Verifiable
- Requirements shall be clearly identifiable
 - Separate requirements from explanatory text
 - Tables are more difficult to verify
 - Pictures are very difficult to verify

How detailed should a requirement be?



Example: Requirement Detail

- The device shall detect air bubbles $>10 \mu\text{l}$ with a sensitivity of $1 \mu\text{l}$. The detection time shall be less than 20 msec.
 - Can be tested using very few test cases
- The device shall detect sufficiently shall air bubbles quickly
Can this be tested? When are you done testing?

'Good' Requirements

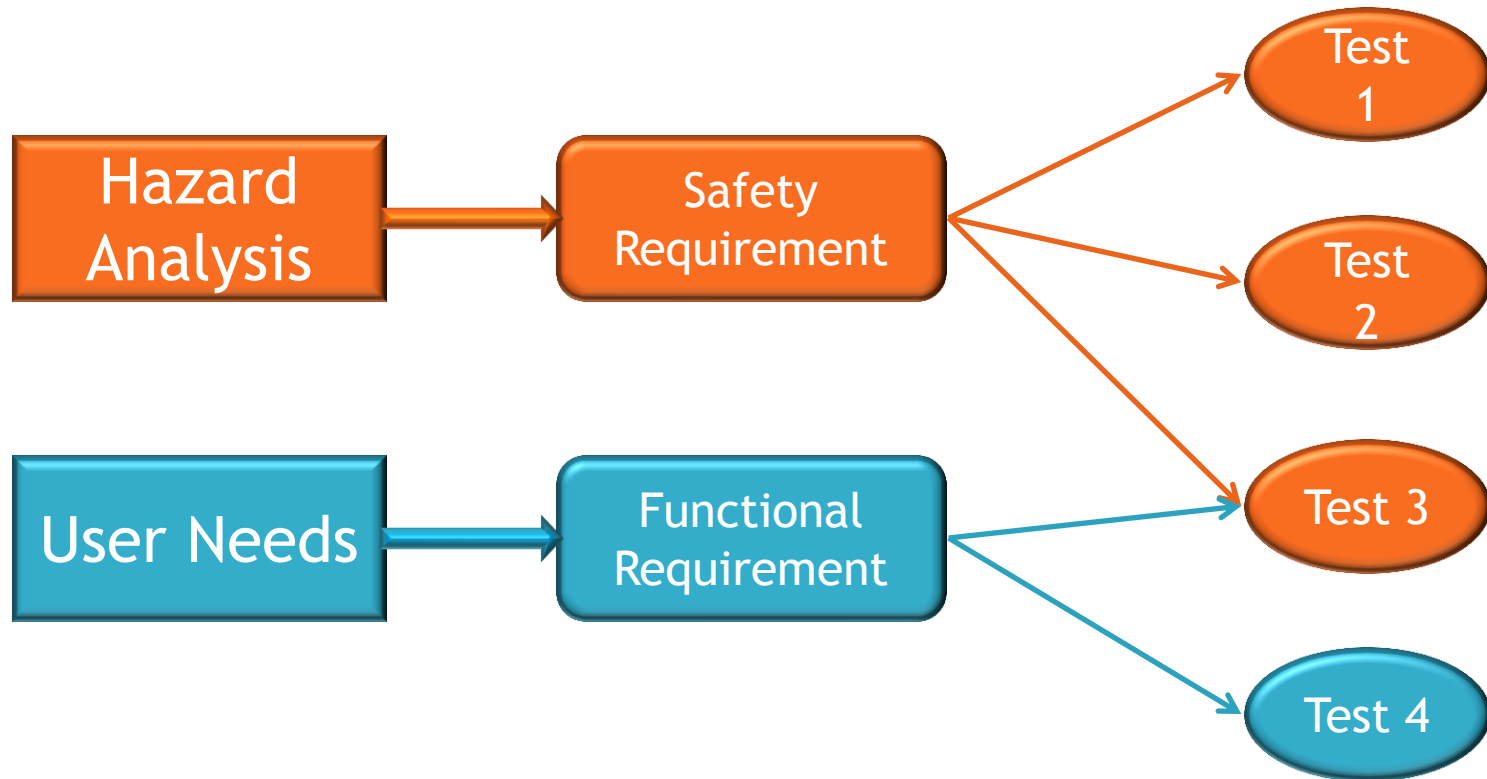
- Complete
 - Fully describe the required function including boundary conditions and exceptions
- Correctness
 - Correctly describe the required function, avoid ambiguity
- Consistent
 - Requirement don't contradict each other
- Clear
 - Requirements are understandable – no implicit assumptions
- Verifiable / Testable
 - The requirement can be verified / tested

'Bad' Requirements

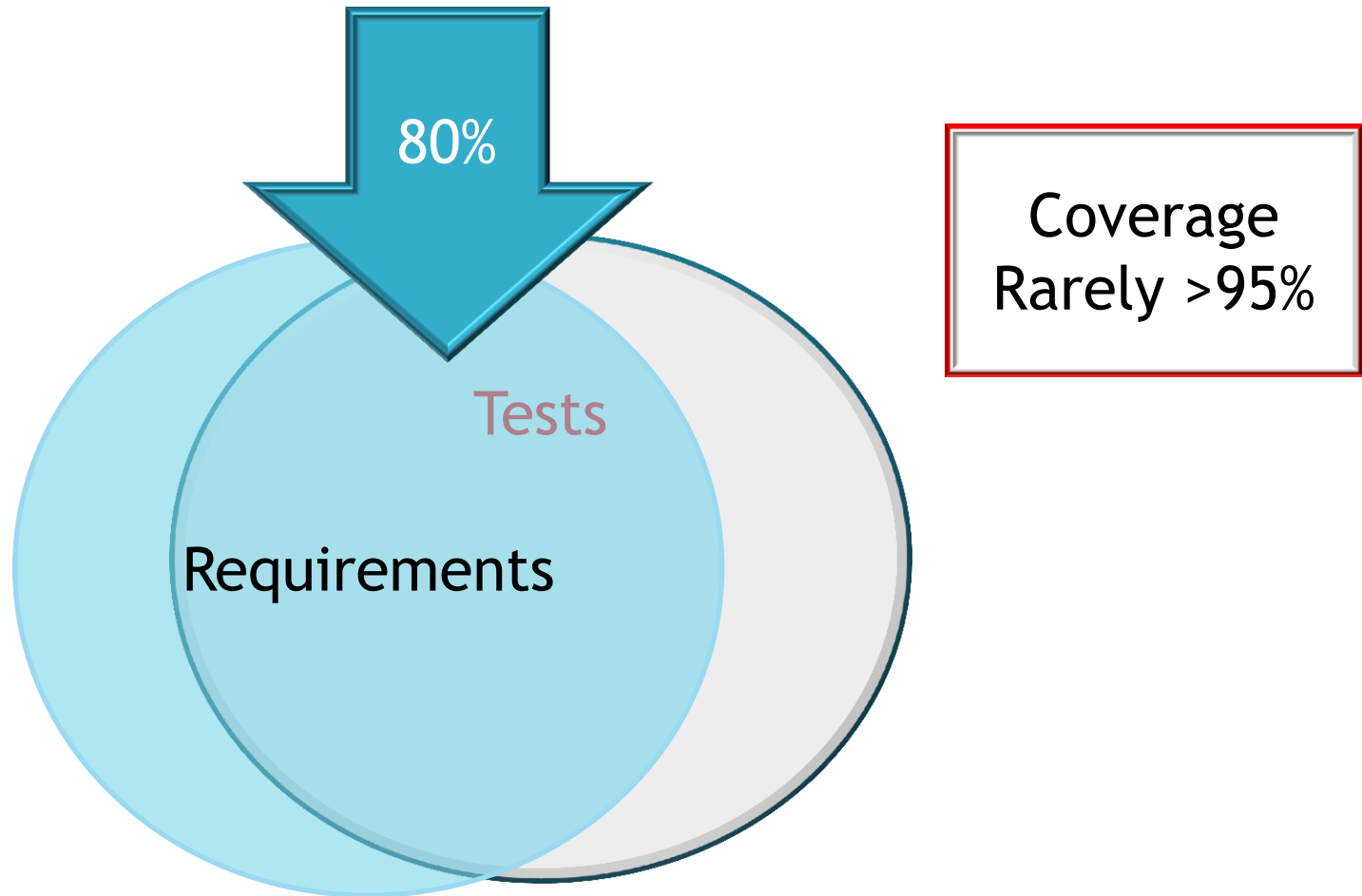
- Incomplete
 - “The device shall detect ambient light conditions.”
 - What are ambient light conditions?
 - What happens based on the detection?
- Ambiguous
 - Terms like ‘easily’, ‘intuitive’, ‘pleasing’
 - Can not be objectively verified
- Unclear
 - “The device shall measure the energy with an accuracy of 2%”
 - Relative? Full scale? Boundaries?

The Quality of the Requirements determines the Quality of the Verification

Requirements Traceability



Test Coverage



Traceability

- Hazard (n)
 - Mitigations ($m*n$)
 - Requirements ($l*m*n$)
 - Test cases ($k*l*m*n$)
 - Test report ($j*k*l*m*n$)

Verification and Validation

- Amount of Rigor for Safety Requirements
- Traceability
- Big three “C”s
 - Completeness
 - Correctness
 - Coverage
- FIT (Fault injection testing) / Stress testing

Testing

- **Requirements based testing (Pass/Fail)**
- Usability testing
- Robustness testing (HART, Environmental, EMC)
- Standards based testing (EN60601)
- Challenge testing

Testing (SRG 1998)

- fault, alarm, and hazard testing
- error, range checking, and boundary value testing
- timing analysis and testing
- special algorithms and interpretation tests and analysis
- stress testing
- device options, accessories, and configurations testing
- communications testing
- memory utilization testing
- qualification of off-the-shelf software
- acceptance and beta site testing
- regression testing

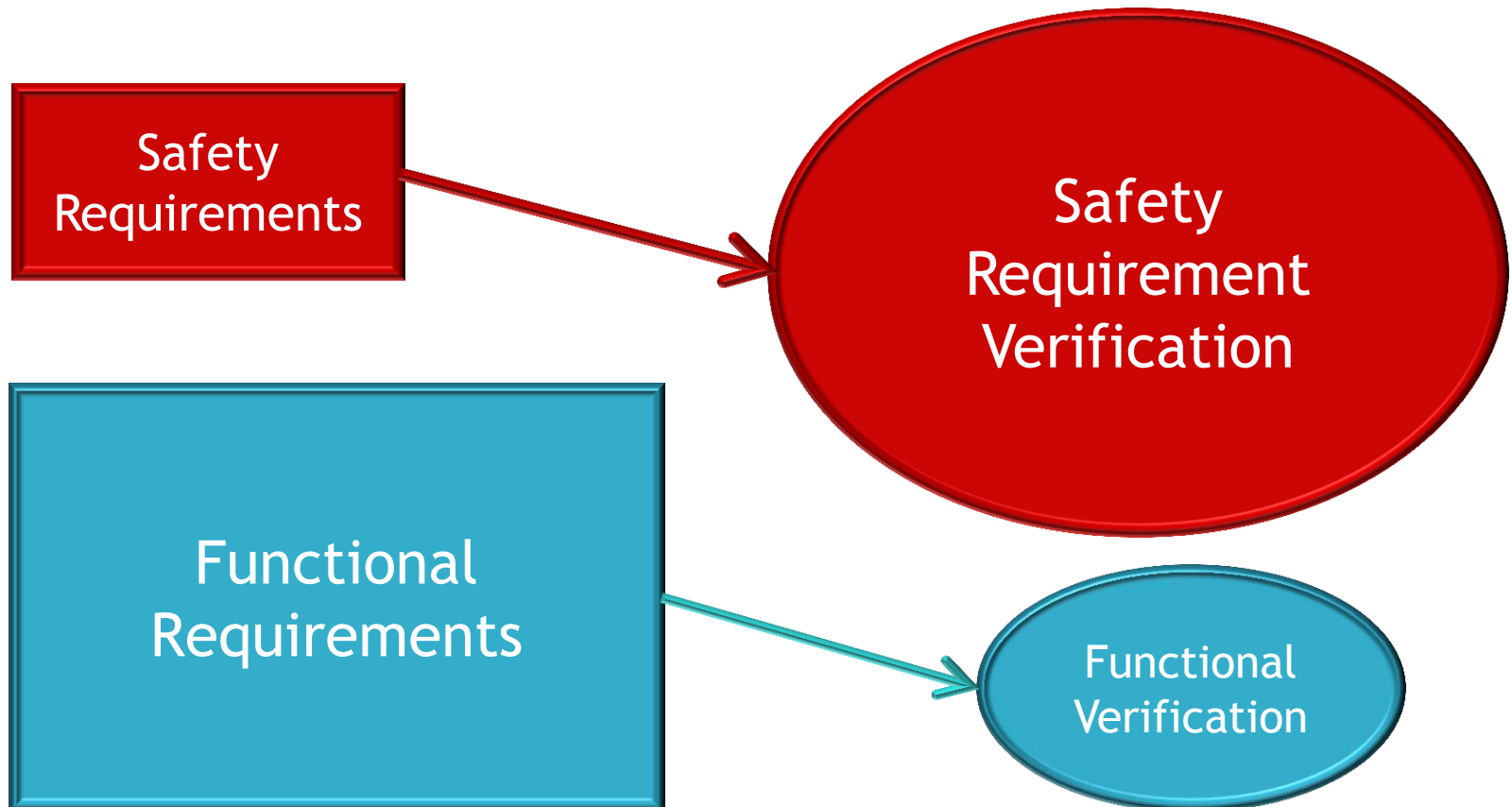
Analysis

- FMEA (Failure Mode and Effects)
 - Qualitative
 - Quantitative
 - FMEDA / FMECA
- Simulation
- Markov Models

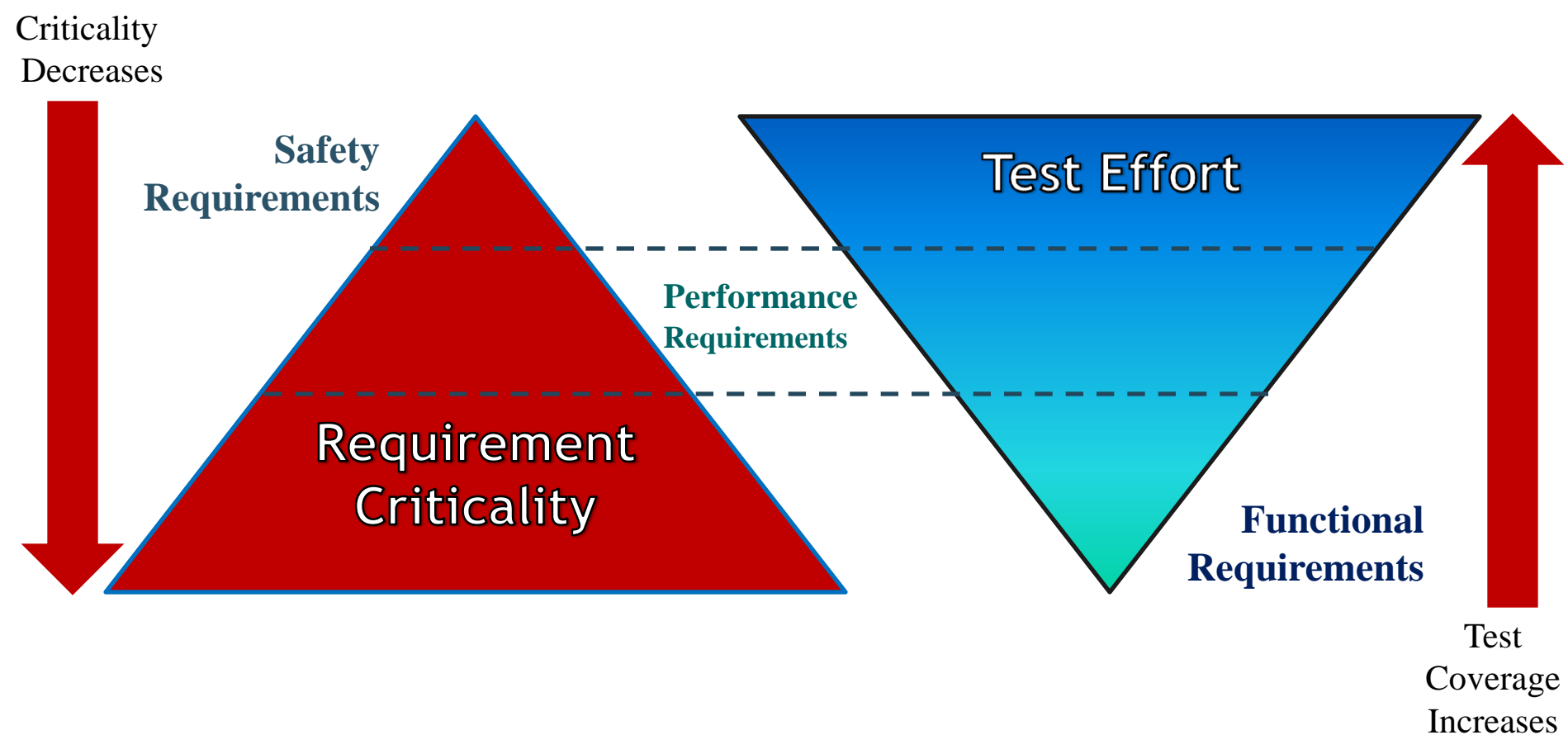
Inspection

- Warnings and Labels
- User Documentation
- Technical Documentation
- Training Material
- Visible and audible device properties

Risk Based Verification



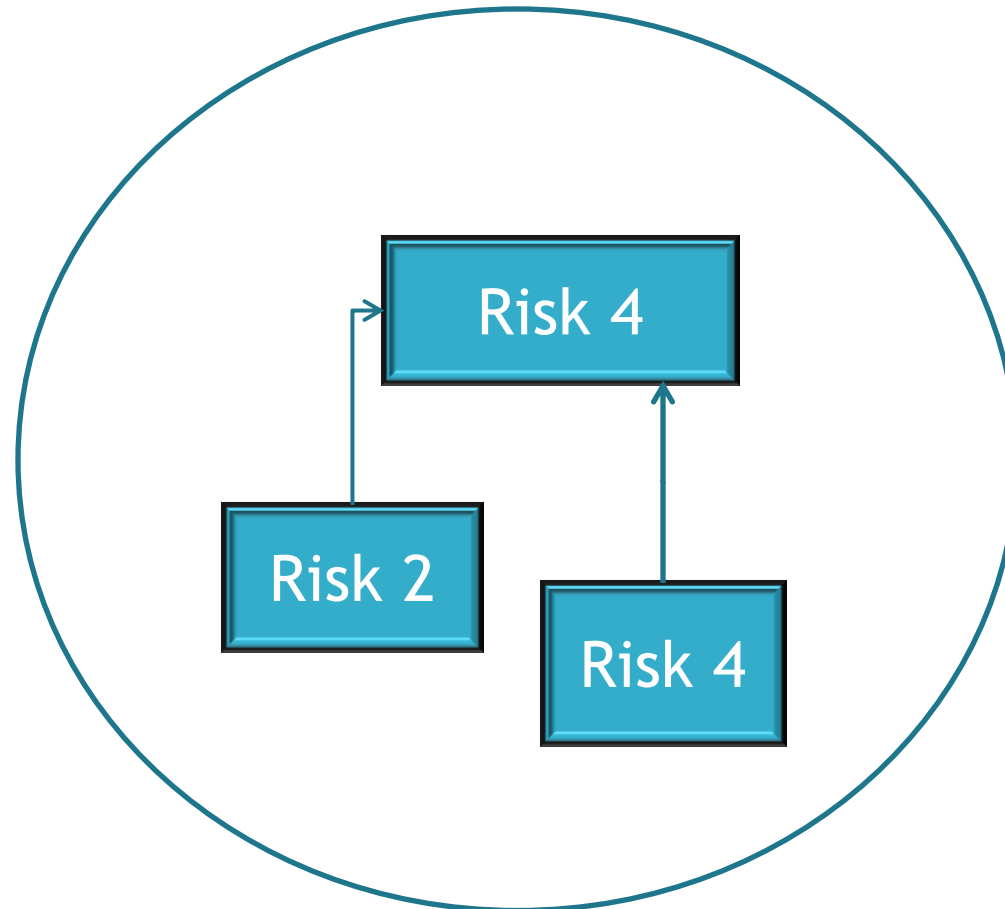
Risk Based Verification



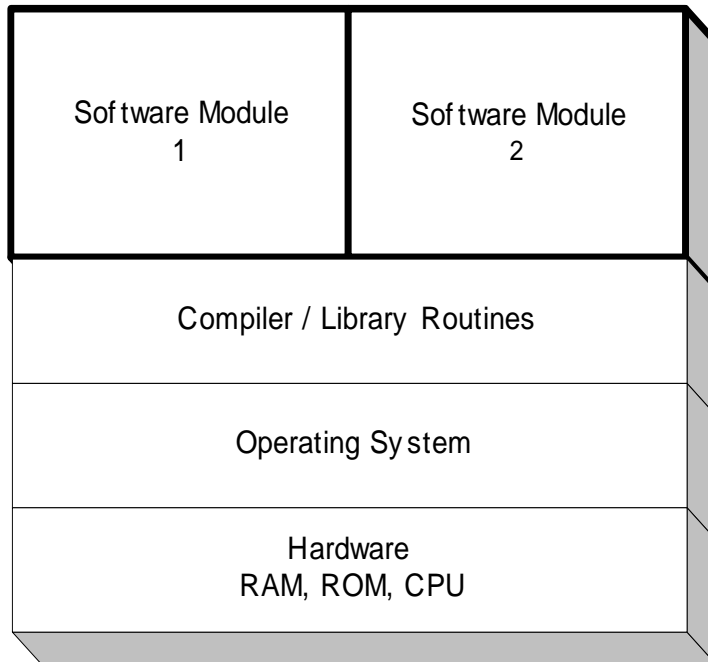
Risk Inheritance

- **IEC 62304:** When a SOFTWARE SYSTEM is decomposed into SOFTWARE ITEMS, and when a SOFTWARE ITEM is decomposed into further SOFTWARE ITEMS, such SOFTWARE ITEMS shall inherit the software safety classification of the original SOFTWARE ITEM (or SOFTWARE SYSTEM) unless the MANUFACTURER documents a rationale for classification into a different software safety class. Such a rationale shall explain how the new SOFTWARE ITEMS are segregated so that they may be classified separately.

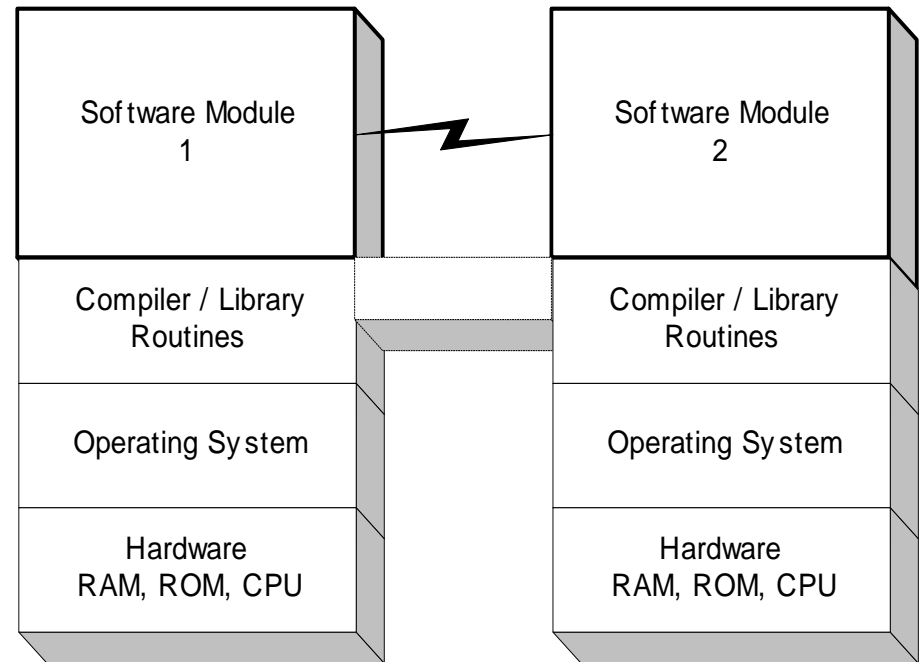
Risk Inheritance



Interference



Software System on
Common Platform



Software System on
Distributed Platform

Interference

- If risk based verification is employed:
 - Test for interference between non-risk components and risk components:
 - Memory
 - Power Supplies, communication lines
 - Shared resources (CPU time, cooling fans, bus systems)

Facilitate Risk Based Verification

- Stratify Requirements
 - Safety Requirements (incl. usability)
 - Performance Requirements
 - Functional Requirements
- Develop Criticality based Verification Activities
 - Safety -> 99% coverage
 - Performance -> 90% coverage
 - Functional -> 60% coverage

Residual Risk

■ Unmitigated Risk

- Inadvertent RF energy output

- Severity = 4, Probability = 4, Risk = $4 * 4 = 16$

■ Mitigations implemented

- Independent RF indication tone and surgeon lifting the pencil

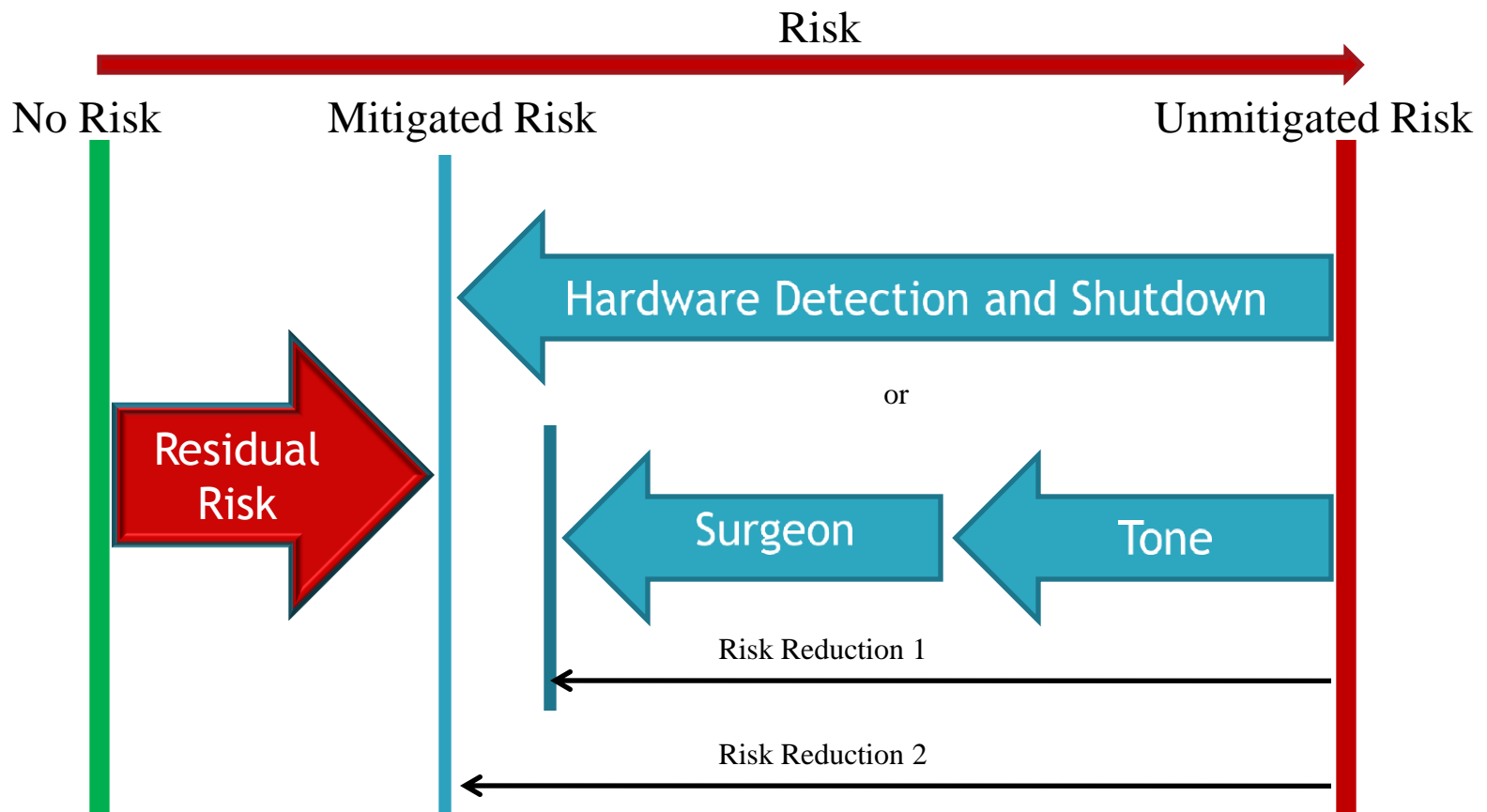
- or

- Hardware monitoring of RF output and shutdown of energy

Residual Risk

- Risk reduction by lowering probability or severity
 - Severity = 4, Probability = 2, Risk = $4 * 4 = 8$
 - Risk reduction by factor 2
 - Remaining (residual) risk is not 0
- Residual Risk (per hazard) is the remaining Risk after all possible / practical mitigation measures are exhausted

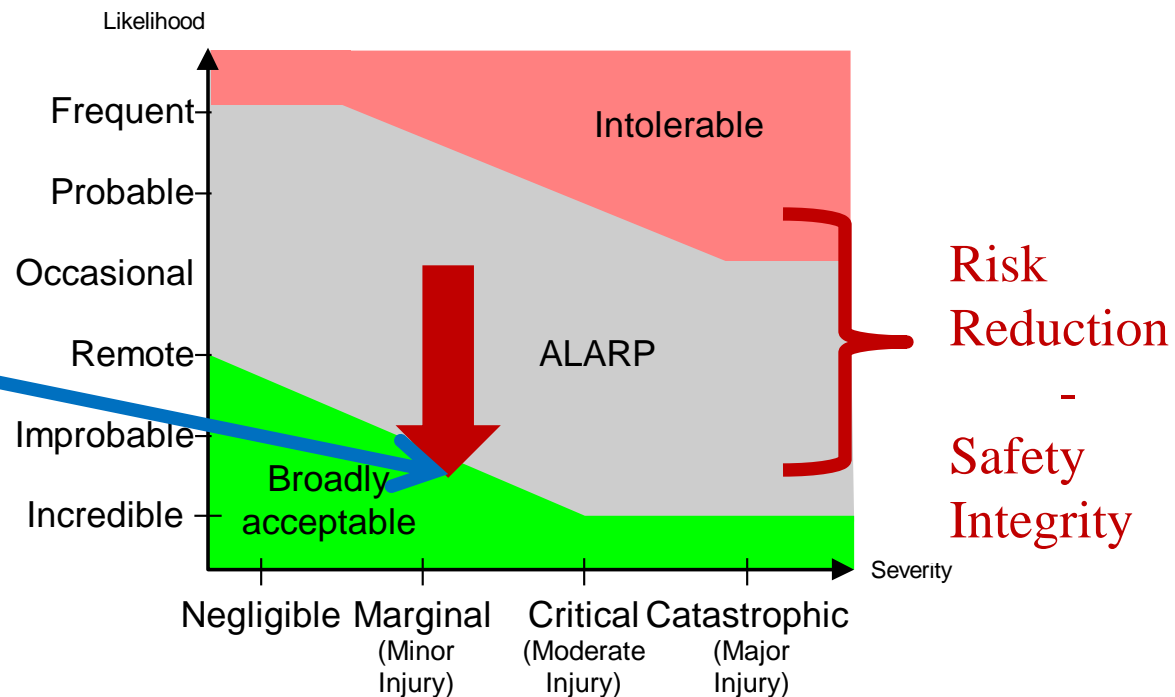
Residual Risk



Residual Risk

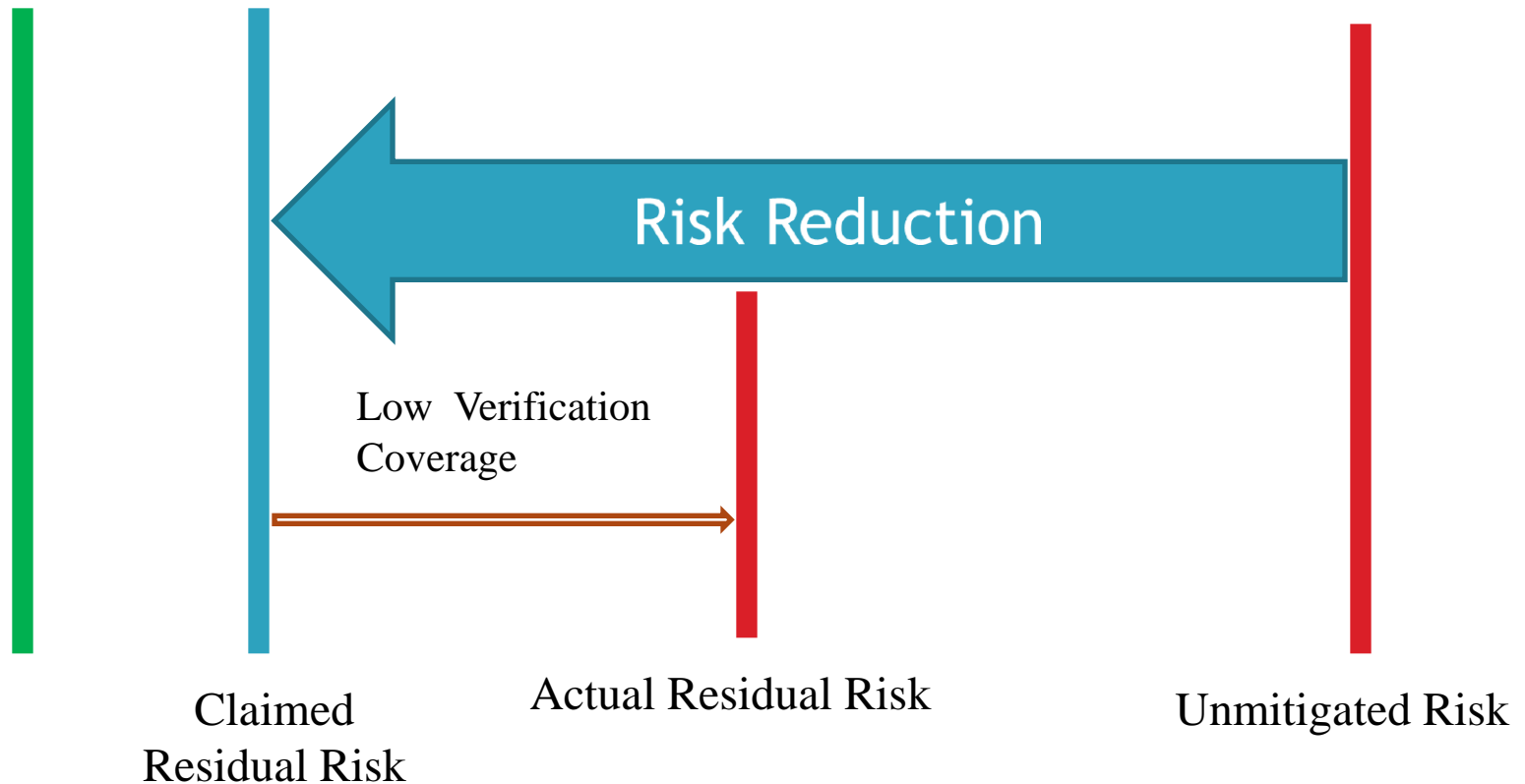
- Commonly define the Risk associated with each identified hazard AFTER mitigations

Residual Risk



Residual Risk Uncertainty

No Risk



Tips and Tricks

- Classify and distinguish requirements based on origin (hazard analysis, user needs ...)
- Clearly identify all safety requirements, implementation subsystems (i.e. air bubble sensor)
- Perform a testability review of all requirements
- Estimate the coverage rate of each verification activity
- Adjust the coverage rate to the criticality of the requirement

Questions

- If there are any further questions which we were not able to get to today please feel free to contact me through Global CompliancePanel



Upcoming Webinar from Markus Weber

- The Recorded Version of this webinar (streaming) is available from Global Compliance Panel.
- Upcoming Live Webinar :
 - ***“Effective Hazard Analysis to meet FDA and ISO13485:2003 Risk Management Requirements”*** on Tuesday, August 30, 2011 at 10:00 AM PDT | 01:00 PM EDT

Past Webinars from Markus Weber

- Recorded Webinars :
 - *Risk Management during device design according to ISO14971*
 - *Hazard Analysis - A practical guide*
 - *Hazard Analysis vs. FMECA - Differences and Commonalities*

- Please Use this link for additional information -
http://globalcompliancepanel.com/control/speakerprofile?speaker_id=10142



Contact Us:

- **Customer Support at**
1.800.447.9407
- **Questions/comments/suggestions**
webinars@GlobalCompliancePanel.com
- **Partners & Resellers:**
partner@GlobalCompliancePanel.com