

A Practical Guide to Hazard Analysis for Medical Devices as required by IEC60601 and ISO14971

Markus Weber
System **S**afety, **I**nc.

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.

© 2009 by System Safety, Inc. All rights reserved. Reproduction in whole or in part without written permission is prohibited.

Purpose

- ▶ Help in streamlining the Hazard Analysis process
- ▶ Help in preparing, organizing and moderating hazard analysis meetings
- ▶ Provide tools to gain maximum benefit for the risk management process
- ▶ Not – citing standard clauses or reiterating issues the standard already addresses

Why Hazard Analysis?

- ▶ It is required by FDA / CE mark for most devices (ISO 14971 and IEC60601-1-4)
- ▶ It helps to design a better (safer) product
- ▶ It makes the developers risk-aware
- ▶ It helps avoiding costly mistakes
- ▶ It documents risk awareness and mitigation
- ▶ It may save your company

Risk Management

Process of

- ▶ identifying,
- ▶ reducing,
- ▶ and managing

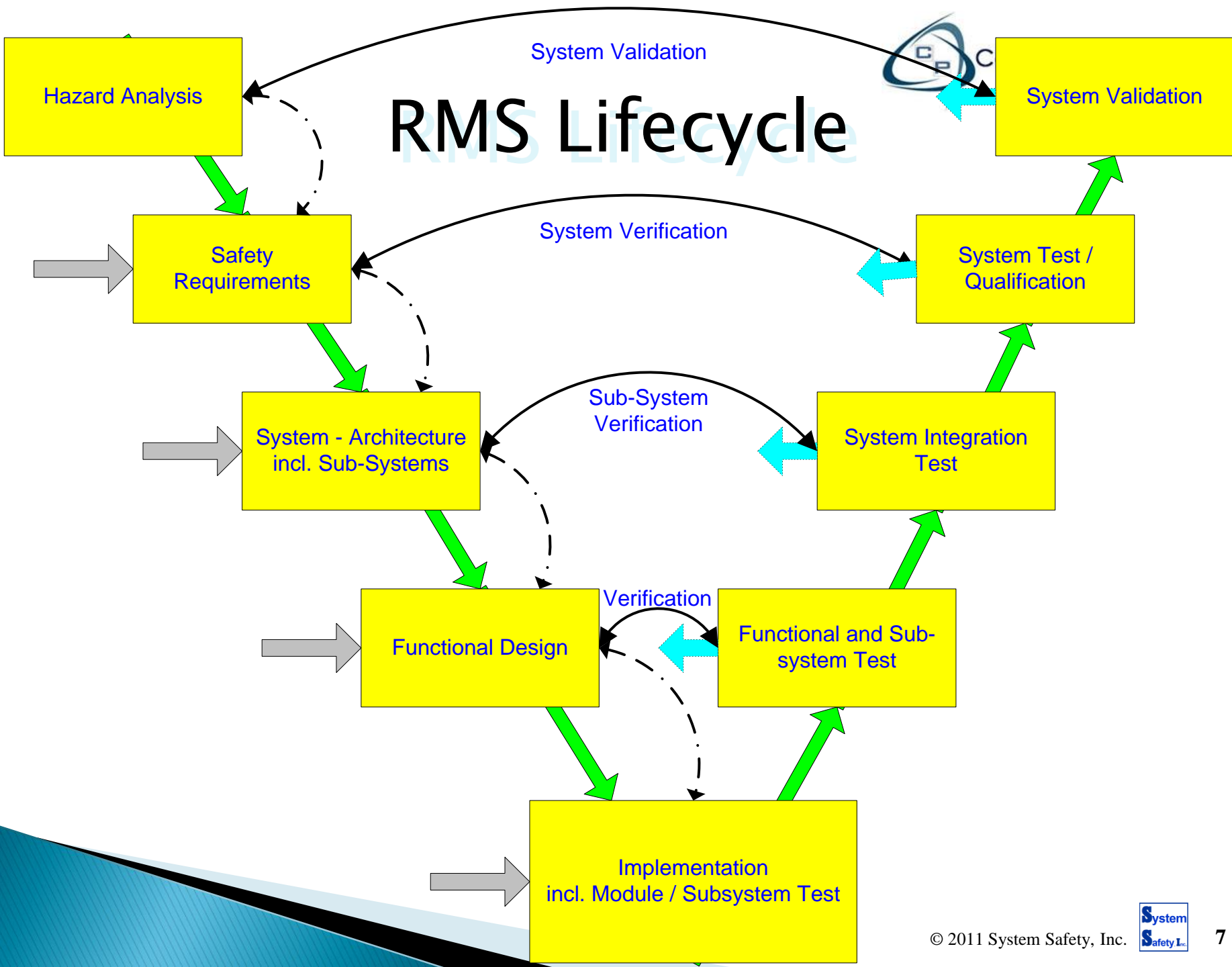
risk throughout the device development and deployment (the entire product life cycle).

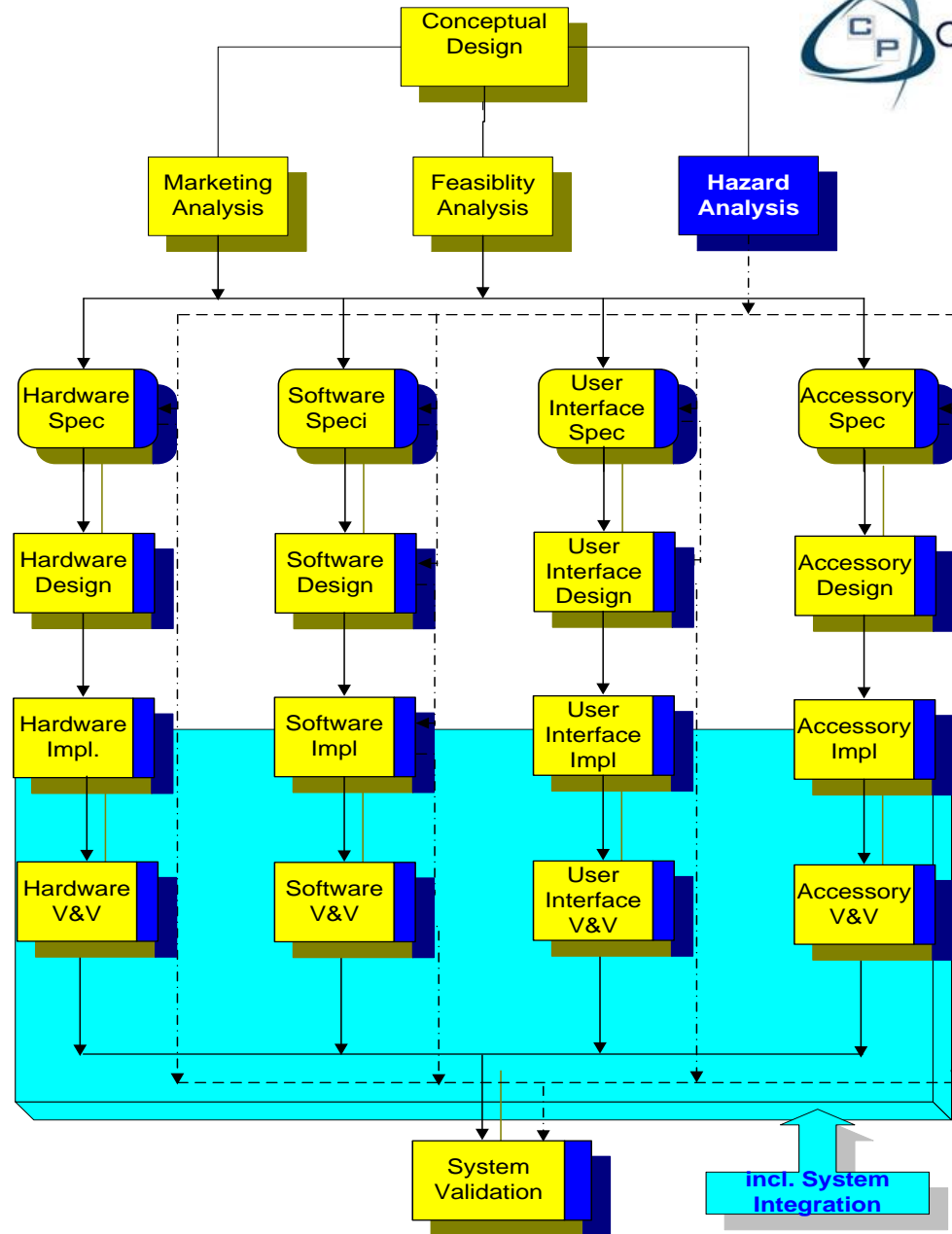
Hazard Analysis covers the first two items.

Risk Management Plan / SOP

- ▶ Draft before hazard analysis
- ▶ Define lifecycle
- ▶ Define responsibilities
- ▶ Define documentation
- ▶ Define corrective actions
- ▶ Define milestones and transfer criteria

RMS Lifecycle





Hazard Analysis Preparation Team Composition

- ▶ Not only developers - include
 - Management
 - Clinical
 - Engineering
 - Service / Marketing
 - Human Factors
 - Legal
- ▶ Invite and provide pre-meeting information
 - Scope
 - Methodology
 - “Framework”

Hazard Analysis

- ▶ NOT a one-time activity but an ongoing process
 - Revisit the Hazard Analysis multiple times during design, implementation, verification and life of the device
 - Documents the maturity of the RM process
 - Should be available to ALL team members
 - Various functions should be able to request review
 - Review results have to flow back into development / manufacturing / service / training

Hazard Analysis Preparation

Scope Definition

- ▶ **Clinical Boundaries**
 - Inclusion criteria
 - Exclusion criteria
- ▶ **Physical Boundaries**
 - Mains connection / grid
 - Connected devices
- ▶ **Implicit Assumptions**
 - Sabotage / maintenance / installation
 - User skill

Hazard Analysis Preparation

- ▶ Define as much information as possible before the first meeting
- ▶ Define Scope, Use environment, Qualitative and Quantitative Properties
- ▶ Set up risk rating schema including probability and severity ratings
- ▶ Identify hazard groups (inclusion and exclusion) like energy, environment, biologics, user environment

Hazard Analysis Preparation

- ▶ Define use environment
 - Environmental conditions
 - User type (Nurse, M.D., Tech, ...)
 - User environment (ER, Ambulatory, Patient controlled)
- ▶ Identify Past problems with Similar Devices
 - ECRI, MDR, MAUDE
 - Standards
 - Scientific and non-scientific articles
 - Experience

Qualitative and Quantitative Properties of Planned Device

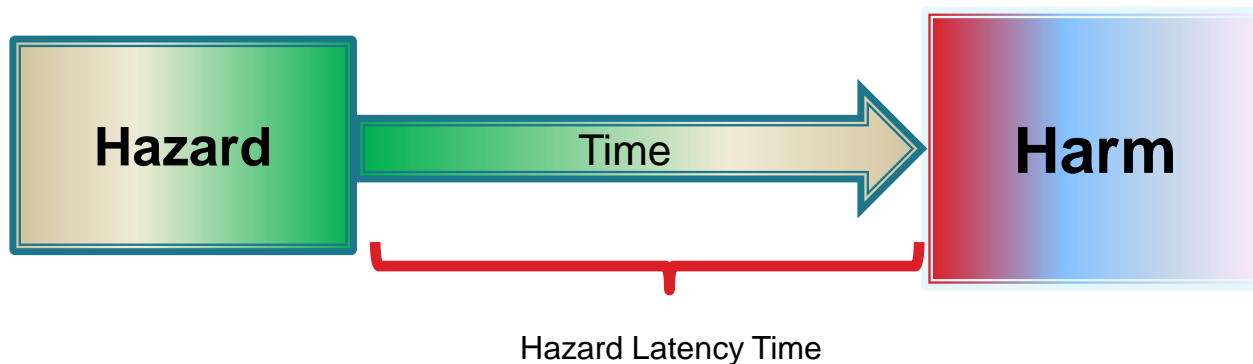
- ▶ Describe the properties of the product
- ▶ Use the guidance provided in ISO14971
 - Formally answer all questions
- ▶ Identify potential properties NOT covered by the ISO questionnaire

What is a Hazard / Cause of a Hazard?

- ▶ Provide a definition of Hazard vs. Hazard Source
- ▶ Difficulty to identify level at which a hazard is defined:
 - Cell hypoxia
 - Loss of blood circulation
 - Cardiac fibrillation
 - Electric shock
 - Loss of mains isolation
 - Degradation of isolation material
- ▶ Hazard: Harm after latency time and lowest clinical level
- ▶ Hazard Cause: Highest technical / organizational level

Hazard Cause, Effect and Harm

- ▶ Hazard is a potentially harmful event that, if not avoided or mitigated, will cause Harm
- ▶ Most hazards have a distinct cause



Hazard Characteristics

- ▶ Resulting Harm
- ▶ Hazard latency time
- ▶ Hazard cause
 - Hazard cause grouping like ISO14975:
 - Energy hazards
 - Biological and chemical hazards
 - Operational hazards (Functional)
 - Information hazards (Labeling)
- ▶ Observability

Hazard Identification

- ▶ Scope of Analysis
- ▶ Identification of unmitigated hazards
- ▶ Identification of potential hazard sources (cause analysis)
- ▶ Grouping and structuring hazard list (use ISO14971)
- ▶ Multiple hazards / multiple causes
- ▶ Chain-of-event hazards

Narrow Hazard Domains

- ▶ **Examples of energy hazards**
 - **Electromagnetic energy**
 - Line voltage
 - Leakage current
- ▶ **Examples of biological and chemical hazards**
 - **Biological**
 - ~~Bacteria~~
 - ~~Viruses~~
- ▶ **Examples of operational hazards**
 - **Function**
 - Incorrect or inappropriate output or functionality
 - ~~Incorrect measurement~~

Standards and Hazards

- ▶ Mitigations covered by standard requirements can or cannot be included
- ▶ Assessment of additional hazards within the standard requirements is necessary
 - E.g. IEC 60601-1 3rd edition
 - Adherence to standards may imply that all hazards are sufficiently mitigated (e.g. IEC 62355 – usability)
- ▶ Standards may require certain Risk Management Activities
 - E.g. IEC 62304 – review of hazard analysis after SRS

Hazard and Risk

$$\text{Risk} = \text{Severity} * \text{Probability}$$

		Severity			
		I Catastrophic	II Critical	III Marginal	IV Negligible
Likelihood	A – frequent				
	B – probable				
	C – occasional				
	D – remote				
	E – improbable				
	F – incredible				

Hazard Analysis Meeting

- ▶ Moderator (also keeps time per item)
 - Allowed or not allowed to actively participate
- ▶ Scribe
 - Projector
- ▶ Group members

Hazard Analysis Meeting

- ▶ Moderator tasks
 - Prepare “framework”
 - Convince the group that a hazard and risk analysis is a meaningful activity
 - Establish ground rules
 - Convey that everybody in the group is a stake holder
 - Introduce the basic methodology
 - Keep track of time per item discussed
 - If a discussion gets out of hand - defer the item
 - Assign action items

Hazard Analysis Meeting

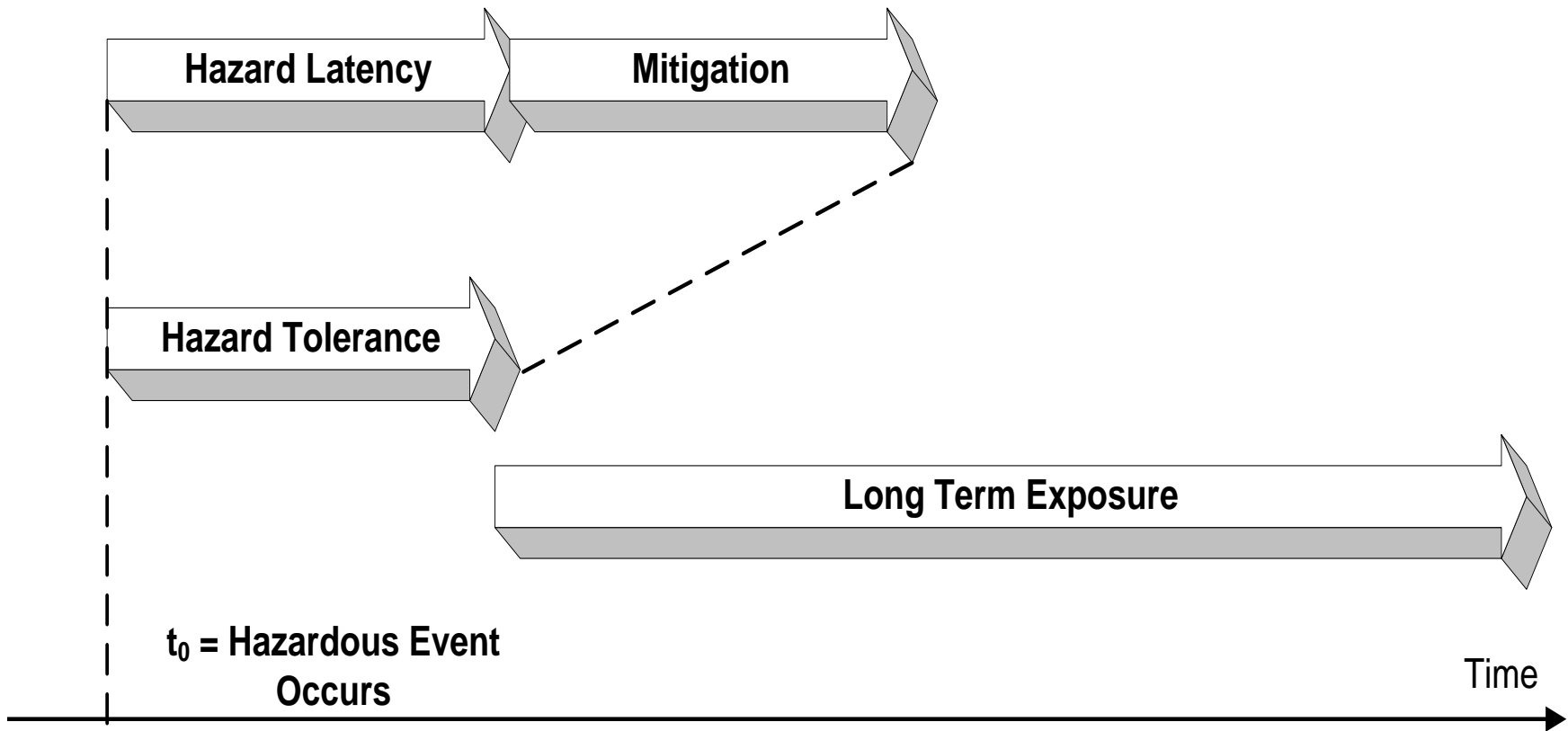
- ▶ Meeting not longer than 4 hours
- ▶ If product complexity requires split into
 - Hazard identification and unmitigated hazard rating
 - Mitigation identification and mitigated hazard rating
 - **Final review**

- ▶ **HAVE WE CAPTURED EVERYTHING?**
- ▶ **ARE WE ALL IN CONSENSUS?**

Hazard Properties

- ▶ Identify hazard / risk characteristics:
 - Severity
 - Probability / Likelihood
 - Observability (of potential hazard – not the event)
 - Latency / Exposure times
 - Risk

Hazard Timing



Determining Risk

Risk = Severity * Probability

Severity = Qualitative

Probability = Qualitative or quantitative

Risk = Qualitative or quantitative

Qualitative vs. Quantitative

- ▶ Only use quantitative assessment if:
 - Data is available to quantify the Probability or Risk
 - Data is verifiable
 - Data is specific to hazard scenario
- ▶ This leaves a qualitative assessment in 99.9% of the cases
- ▶ It is difficult to use mixed categorization in one analysis

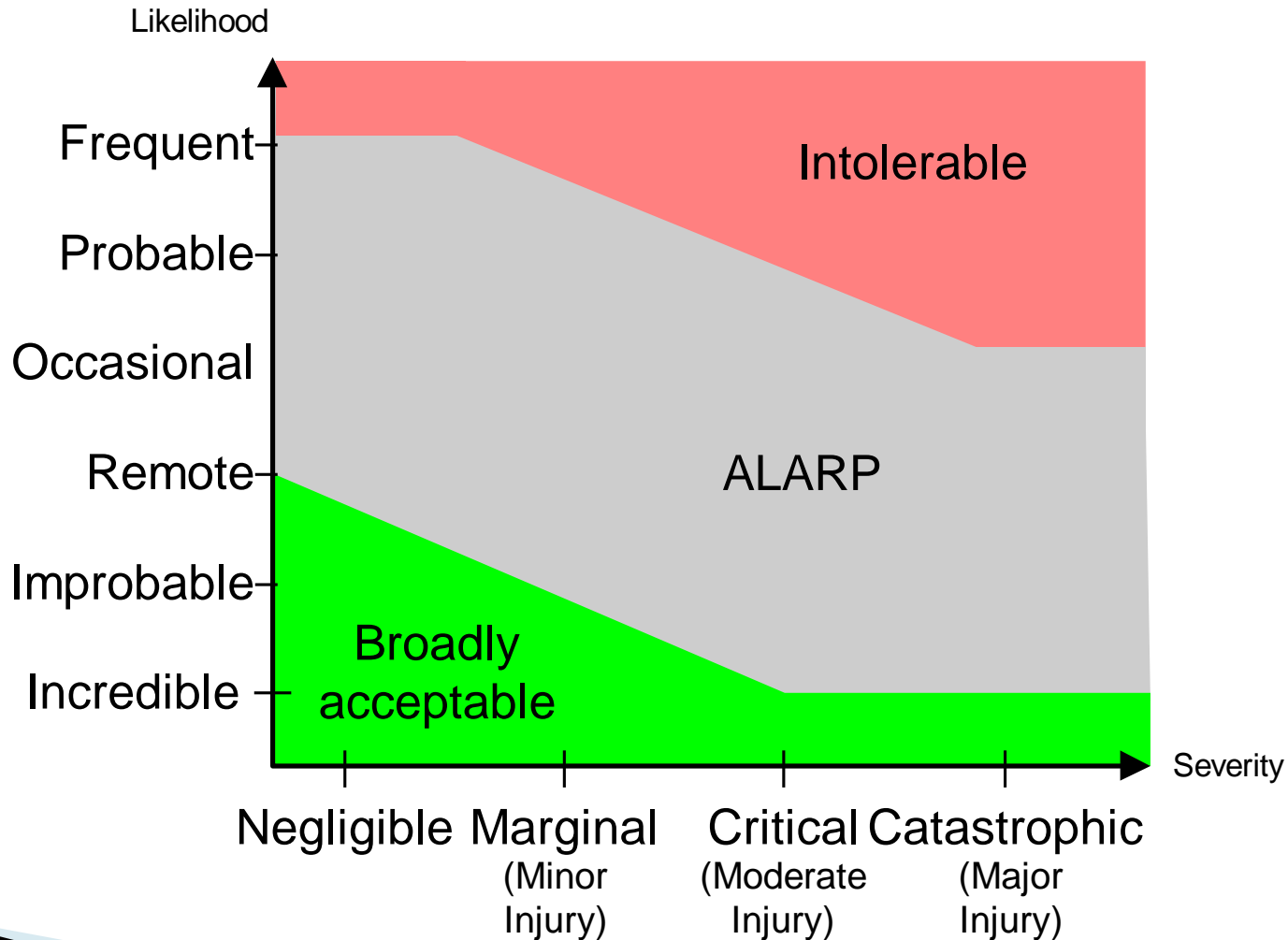
Risk Estimation

- ▶ Risk estimation is an estimate of unmitigated / mitigated risk
- ▶ Unmitigated risk assessment relevant
- ▶ The estimate is not verifiable
- ▶ “Your guess is as good as mine”
- ▶ Consensus on risks relative to each other is more important than the risk “number”

Risk Matrix

	Severity				
		I Catastrophic	II Critical	III Marginal	IV Negligible
Likelihood	A – frequent				
	B – probable				
	C – occasional				
	D – remote				
	E – improbable				
	F – incredible				

The ALARP Principle



Mitigation

- Inherent safe design
 - Risk avoidance
- Risk control / mitigation
 - Instrumented mitigation
 - User measures including alarms
- User information about residual risks

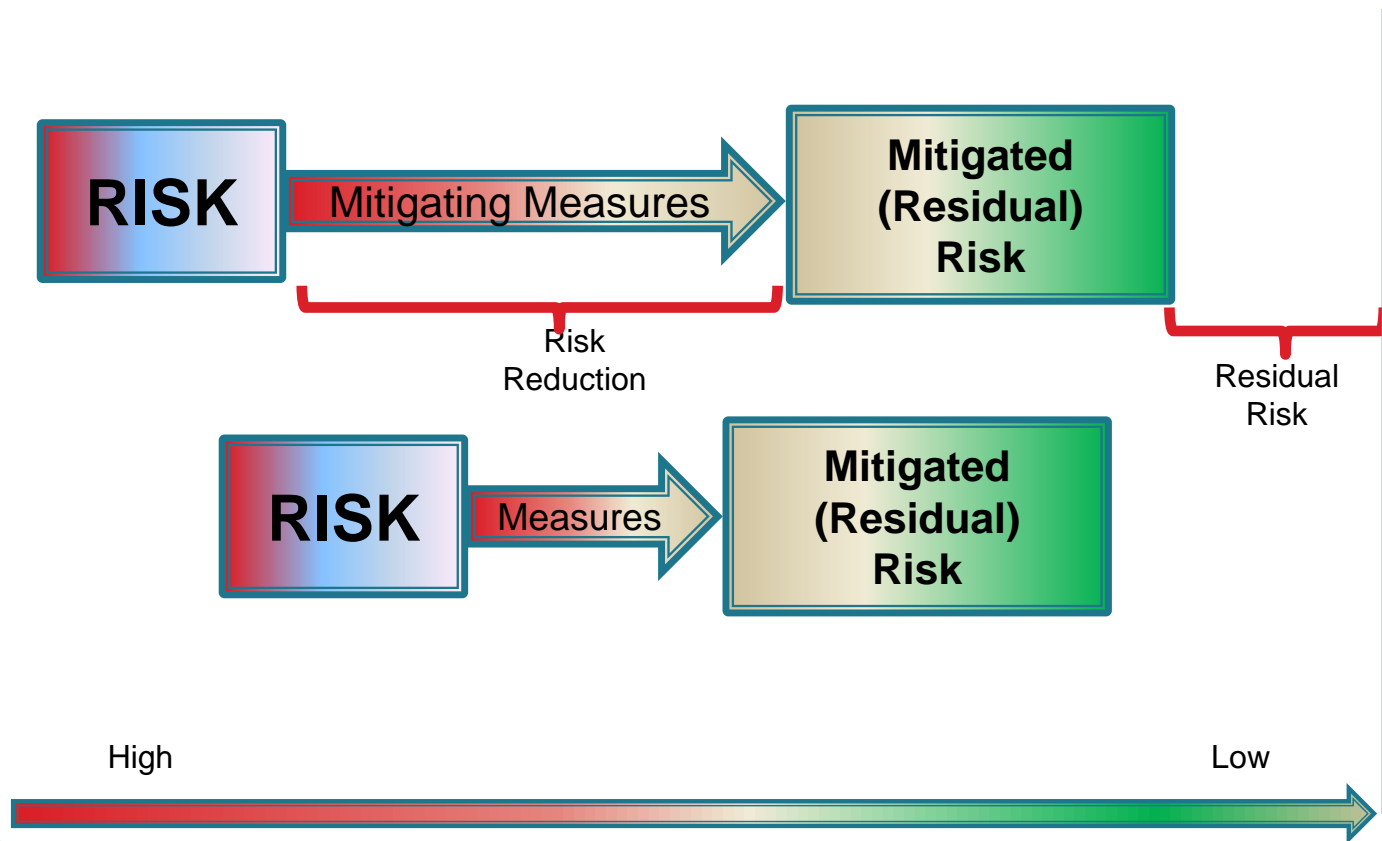
Mitigator Allocation

- ▶ Hardware
 - ▶ Software
 - ▶ Procedure / human action
 - ▶ Combination of above
-
- ▶ Sometimes it is difficult to determine risk reduction of combined mitigations.
 - Define mitigation “bundles”

Post-Mitigation Risk Assessment

- ▶ Estimate the Residual Risk (post mitigation risk) for each hazard
- ▶ If multiple mitigations are used:
 - Rate the risk reduction separately
 - Problem: How to consolidate contributions
 - Rate the combined risk reduction as combination of mitigations
- ▶ The spread between unmitigated and mitigated Risk is the Risk Reduction
- ▶ The Safety Integrity has to reflect the Risk reduction

Risk Reduction



“The TABLE”

1. Energy Hazards and Contributory Factors

Hazard Sub-Domain															
Hazard Sub-Domain	Hazards														
	Hazard	Component	Hazard Description							Control / Mitigation					
			Hazard Description	Hazard Source	Hazard Latency Time	O	L	S	RF	Mitigating Measure	M-L	M-S	RF	M-Risk Rating	Verification Reference
1.1. Electricity	1.1. Electric shock	PS	Leakage current too high	Circuitry - Breach of enclosure	< msec	N	3	4	12	G 6.2, 8.3 - rating against shock of B, BF or CF, or defib-proof	1	4	4	ALARP	

Hazard Analysis Pitfalls

- ▶ Missed hazards
- ▶ False or incomplete hazard identification
- ▶ Overconfidence in the process
- ▶ Misunderstanding / different understanding of hazard cause / effect relationships
- ▶ Omission of low criticality hazards
- ▶ Misunderstanding the use environment

Tips and Tricks

- ▶ Use ISO 14971 as template for your Risk Management SOP
- ▶ Adopt ISO 14971 terminology
- ▶ Appoint a Risk Manager
- ▶ Include a Risk Management Section into every document you produce
 - Specifications
 - Meeting minutes
- ▶ Define trigger events for Hazard Analysis Review
 - E.g. Specification release, release to verification, CAPAs

Tips and Tricks

- ▶ Identify and label safety critical items originating in hazard analysis (components, requirements, software, documentation)
- ▶ Don't be over-confident in the Risk Management Process
- ▶ Use comments in the Risk Analysis Table to document the rationale behind the rating

Potential Problems

- ▶ Missed hazards
- ▶ False or incomplete hazard identification
- ▶ Overconfidence in the process
- ▶ Misunderstanding / different understanding of hazard cause / effect relationships
- ▶ Omission of low criticality hazards
- ▶ Misunderstanding the use environment