Fault Management in an Objectives-Based/Risk-Informed View of Safety and Mission Success

Dr. Frank Groen

NASA Office of Safety and Mission Assurance

NASA Fault Management Workshop

New Orleans, April 10-12, 2012

Traditional SMA Planning

- Bottom up: focus on processes, standards, products
  - Process-based view of technical disciplines
- Limited coordination between disciplines
- Value of individual processes hard to characterize
- Difficult to modify established practices

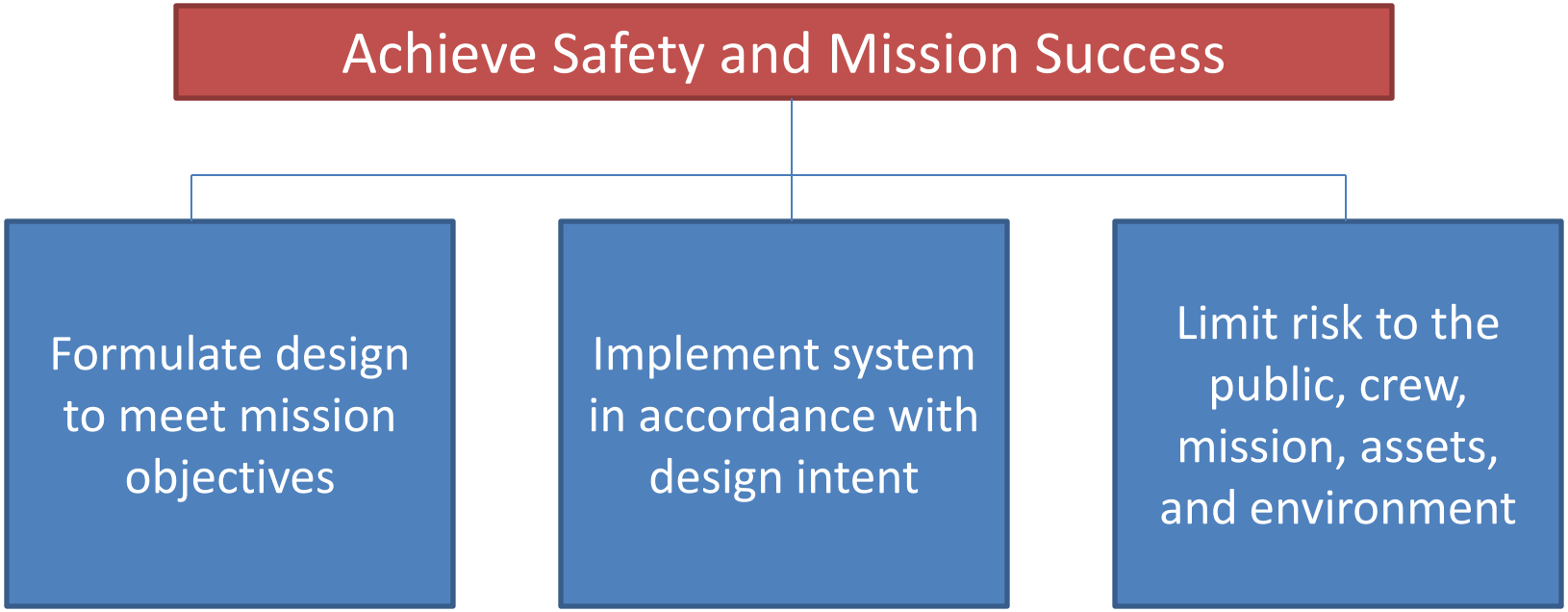
- Lack of clearly-defined, coherent set of objectives based on which adequacy of processes, standards, and products can be measured

Theme of this Talk

- Net-benefit of activities and decisions derives from objectives (and their priority)
  - Similarly: need for integration, value of technology/capability
- Risk is a lack of confidence that objectives will be met
  - Risk-informed decision making requires objectives
- Consideration of objectives is central to recent guidance:
  - Risk Management handbook (NASA/SP-2011-3422)
  - System Safety handbook (NASA/SP-2010-580)

“Safety and Mission Success”

- Possible definition in terms of objectives:



- Programs must establish and maintain confidence that objectives are/will be satisfied

Higher-Level Objectives

- Top-level objectives*:

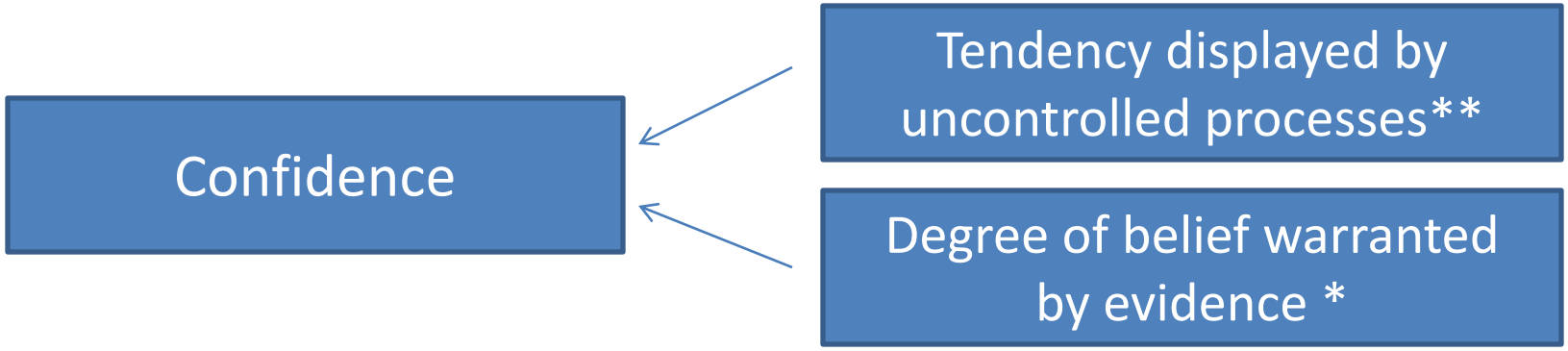
* e.g., NPR 7123.1 and NPD 8700.1

- Abstract objectives must be broken down into more concrete ones (objectives analysis)
  - So they can be asserted with confidence
  - "Dad, let me show you how …"**

**R. Mager

Concept: Confidence and Risk

- Risk originates from a lack of confidence
  - Lack of certainty in ability to achieve objectives



* e.g., see I. Hacking
** must itself be known

- Risk best characterized in terms of:
  - Scenarios by which objectives would not be met
  - Likelihood of those scenarios
  - Consequence (severity) of performance degradation

- Bonus: probability is a measure of degree of belief (Bayes)
  - This includes P(LOC) and P(LOM)

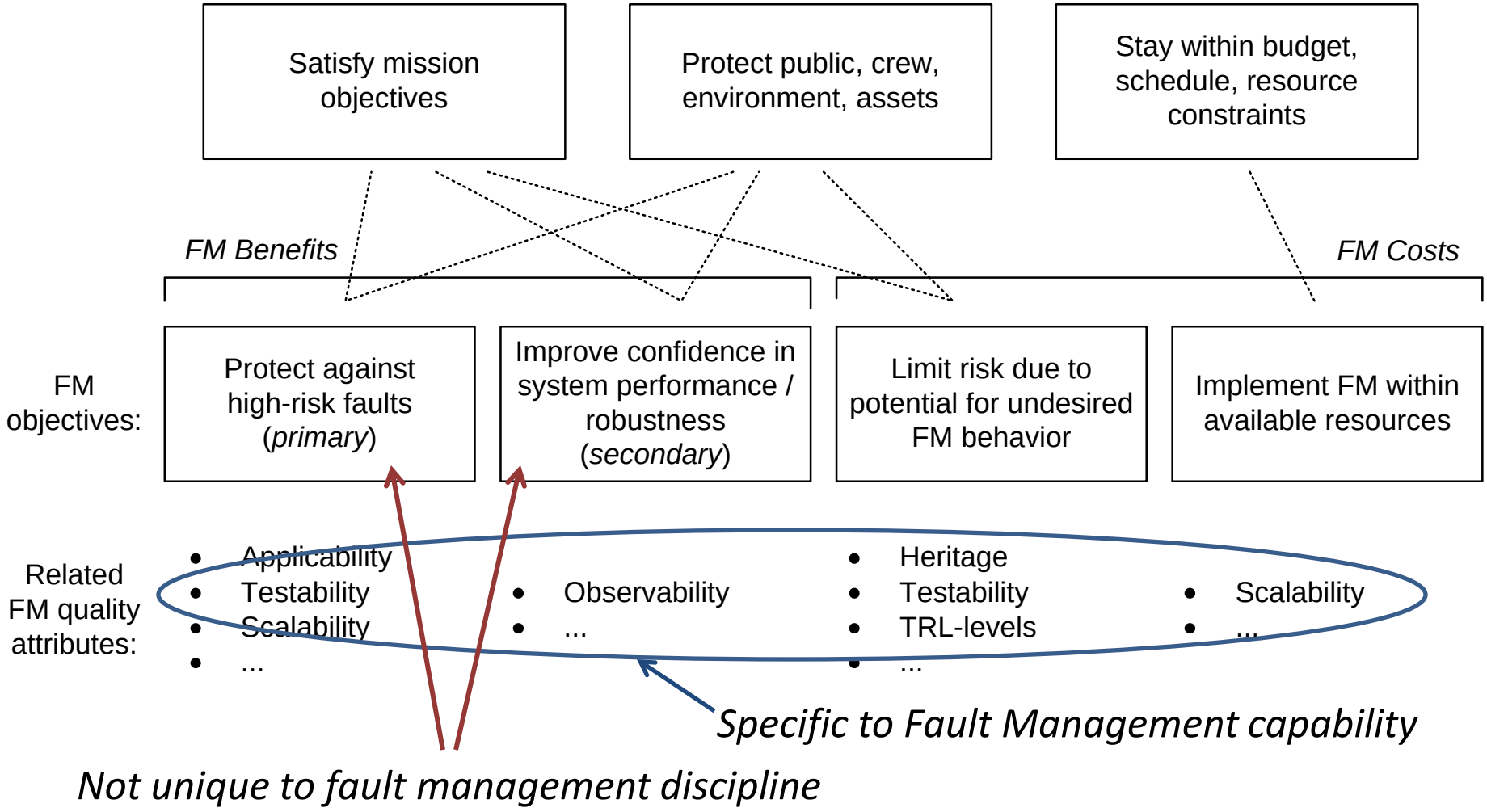
Relevance of Objectives to FM Workshop

- *Identification of FM quality attributes:*
  Objectives provide a basis for determining relevance and completeness of attributes

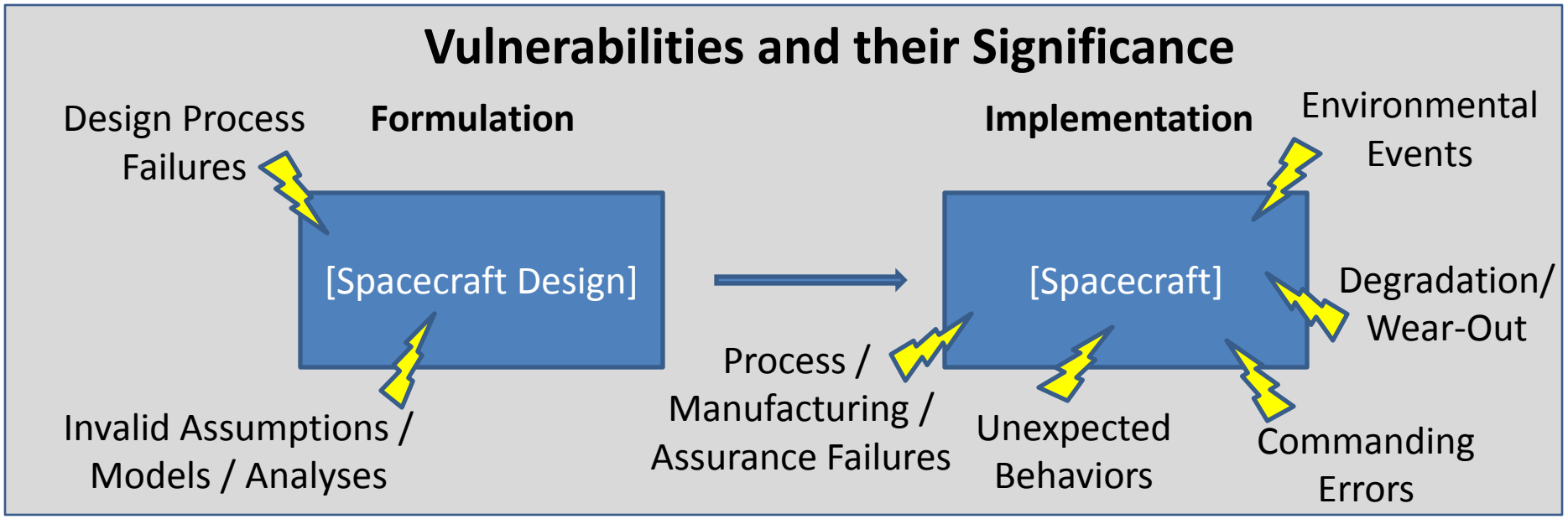
- *Coordination of terminology:*
  Requires shared understanding of objectives

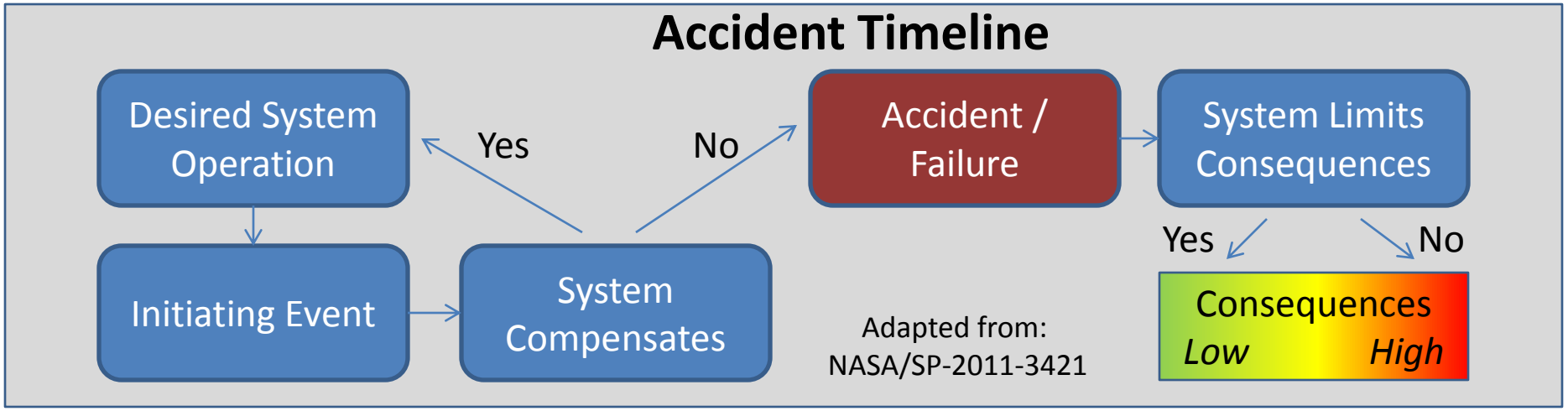
- *Recognition of Fault Management capabilities:*
  Objectives provide outsider perspective on discipline, including overlaps with other disciplines

Isolated View of FM Objectives

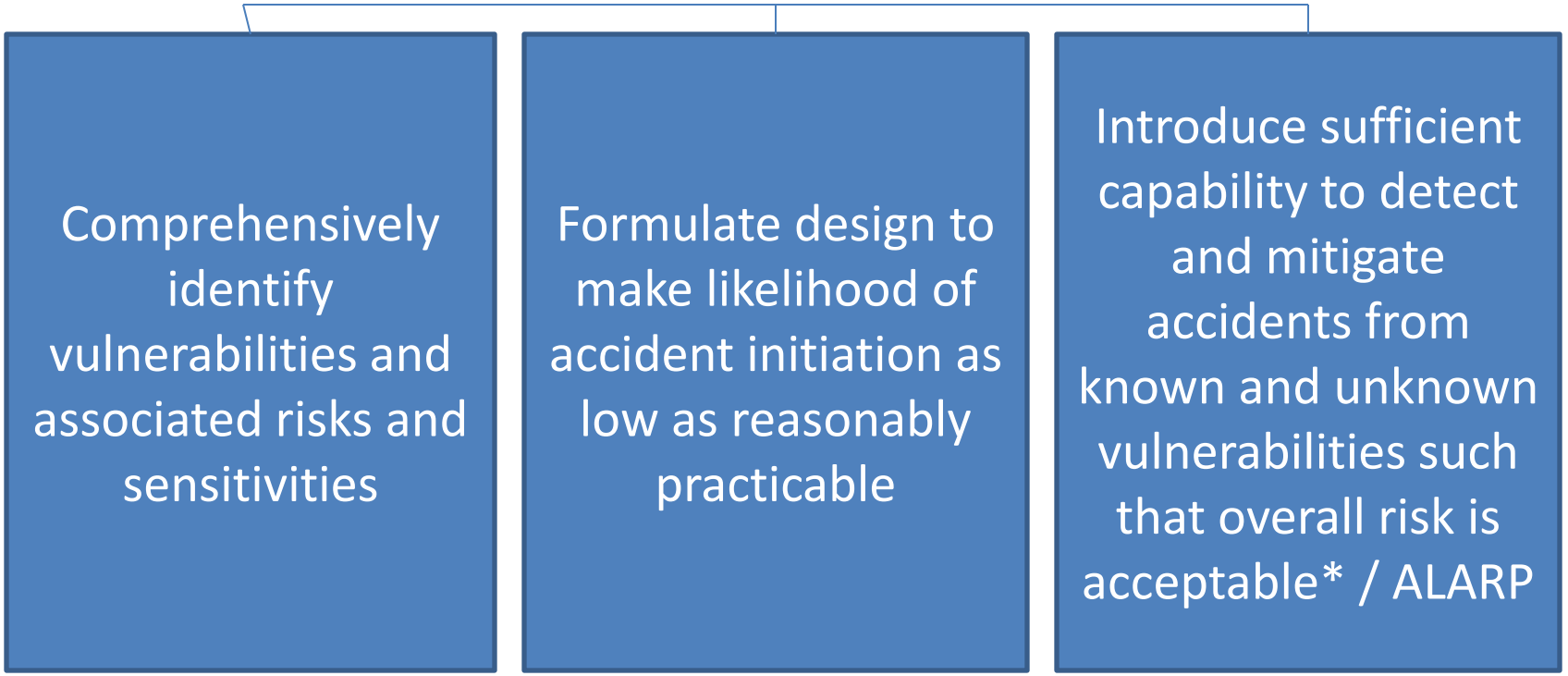


Basis for Coherent SMA/FM Objectives





Breakdown of SMS "Risk" Objectives



- These are common to all disciplines (system safety, reliability, fault mgmt, …), though focus may vary

*E.g., LOC/LOM requirements

Mapping to Common Discipline Activities

- "Formulate design to make likelihood of accident initiation as low as reasonably practicable"

Discipline	Intent of Typical Processes, Standards
Reliability [NS-8729.1]	Operate EEE parts well within rated operating conditions Minimize potential for dielectric discharging; Provide radiation shielding; Provide functional redundancy; …
Software Assurance [-]	[develop using a planned process based, avoid complexity, incorporate ability to handle/recover from contingencies]
System Safety [NPR 8715.3]	Eliminate hazards; Avoid accidents via controls (redundancies, procedures, warnings, …)
Fault Management [FM handbook]	Provide failure detection, fault isolation, failure response determination, and failure recovery mechanisms

- Disciplines should coordinate to ensure coherence
  - Consistent, logical interfaces, complete, no conflicts
  - Objective structures will be interwoven

Concluding Remarks

- Set of SMS objectives are common across all disciplines
- SMS objectives and consideration of associated risks is proposed as a framework for coordinating activities between disciplines
- New system safety paradigm puts greater focus on:
  - Deciding on SMS features in a risk-informed manner
  - Building a case that objectives are met
  - Review of plans and products based on objectives