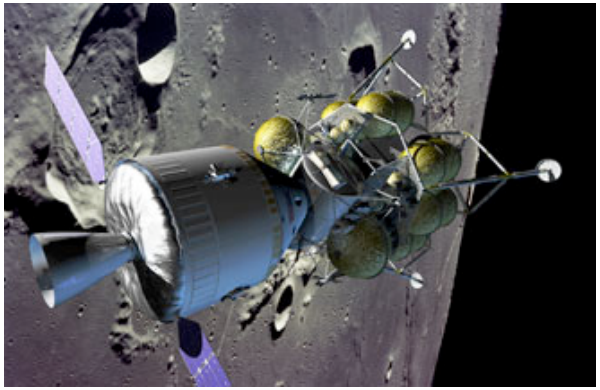
Complex Systems Design
Research Overview

Irem Y. Tumer
Associate Professor
Complex System Design Laboratory
Department of Mechanical Engineering
Oregon State University
irem.tumer@oregonstate.edu

Challenge of Designing Aerospace Systems



Irem Y. Tumer
irem.tumer@oregonstate.edu

Complex Aerospace Systems
Unique Design Environment

- High-risk, high-cost, low-volume missions with significant societal and scientific impacts
- Rigid design constraints
- Extremely tight feasible design space
- Highly risk-driven systems where risk and uncertainty cannot always be captured or understood
- Highly complex systems where subsystem interactions and system-level impact cannot always be modeled
- Highly software intensive systems

Motivation and Research Needs

- *Introducing failure & risk in early design*
  - Analysis of potential failures and associated risks must be done at this earliest stage to develop robust integrated systems
    - Systematic, standardized & robust treatment of failures and risks
- *Enabling trade studies during early design*
  - Early stage design provides the greatest opportunities to explore design alternatives and perform trade studies
    - Reduce the number of design iterations and test & fix cycles
    - Reduce cost, improve safety, improve reliability
- *Enabling system-level design & analysis*
  - Subsystems must be designed as a critical part of the overall system architecture, and not individually or as an afterthought
    - Increase ROBUSTNESS of final integrated architecture
      - Include all aspects of design trade space and all stakeholders
      - Design and optimize as a system

Complex Systems Design

Related Fields of Research

Main Research Thrusts in CoDesign Lab:

- *Model-based design:* Analysis and simulation tools and metrics to evaluate designs, and to capture and analyze interactions and failures in the early conceptual design stages
- *Risk-based design:* Formal process of quantifying risk and trading risk along with cost and performance during early design, moving away from reliance on expert elicitation
- *System-level design:* Multidisciplinary approach to define customer needs and functionality early in the development cycle to proceed with design synthesis and system validation for the entire system

Related Fields:

- Reliability engineering
- Safety engineering
- Software engineering
- Systems engineering
- Simulation based design
- Control systems design

Complex System Design

Formal Methods Research

- Design Theory & Methodology Research (*early design*):
  - Modeling techniques:
    - Function-based modeling
    - Bond graph modeling
  - Mathematical techniques:
    - Uncertainty modeling, decision theory, risk modeling, optimization, control theory, robust design methods, etc.
  - Systematic methodologies:
    - Design for X (mitigation, maintainability, failure prevention, etc.),
    - System engineering methods
    - Axiomatic design, etc.
- Risk and Reliability Based Design Methods (*later design stages*):
  - PRA, FTA, FMEA/FMECA, reliability block diagrams, event sequence diagrams, safety factors, knowledge-based methods, expert elicitation
- Design for Testability Methods (*middle stages*):
  - TEAMS, Xpress

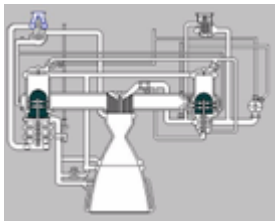
Driving Application
Integrated Systems Health Management (ISHM)

A ***system engineering discipline*** that addresses the design, development, operation, and lifecycle management of subsystems, vehicles, and other operational systems, with the goal of:

- maintaining nominal system behavior and function
- assuring mission safety & effectiveness under off-nominal conditions

Design of Health Management Systems

- Testability
- Maintainability
- Recoverability
- Verification and validation of ISHM capabilities



Real-Time Systems Health Management

- Distributed sensing
- Fault detection, isolation, and recovery
- Failure prediction and mitigation
- Robust control under failure
- Crew and operator interfaces

Informed Logistics & Maintenance

- Modeling of failure mechanisms
- Prognostics
- Troubleshooting assistance
- Maintenance planning
- End-of-life decisions

Irem Y. Tumer
irem.tumer@oregonstate.edu

ISHM State-of-the-Practice

FACT: True ISHM has never been achieved!

System-level

Management: mitigation & recovery

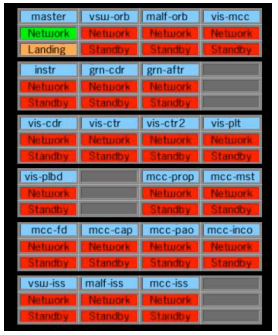
Some Examples at NASA:

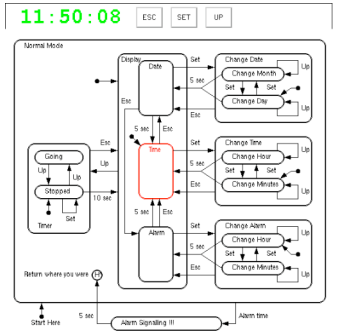
- ISS/Shuttle: Caution and Warning System
- Shuttle: minimal structural monitoring
- SSME: AHMS
- EO-1 and DS-1 technology experiments
- 2GRLV, SLI: Propulsion HM testbeds and prototypes

ISHM sophistication level inversely proportional with distance from earth!

Position	Vehicle	Capability
Mars	MER	Fault Protection
LEO	ISS	Warning System
Ascent to Orbit	SSME	AHMS Redline Cutoff
Atmosphere	JSF, 777	Multi-System Diagnostics, CBM
Ground	Automobile	On-star, ABS, Traction Control

Space Shuttle C&W System





Irem Y. Tumer
irem.tumer@oregonstate.edu

Spacecraft Health Management at NASA

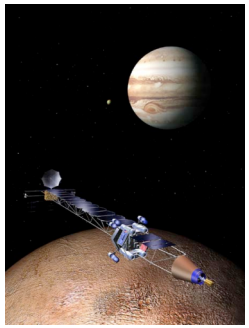
Crew Launch Vehicle ("Ares")

- 1/2,000 probability of loss-of-crew
- Based on legacy human-rated propulsion systems (J2X, RSRM)
- The order-of-magnitude improvement in crew safety comes from crew escape provisions!
- **ISHM focus on sensor selection and optimization, crew escape logic, and functional failure analysis.**

Crew Exploration Vehicle ("CEV")

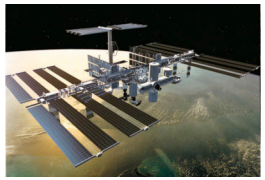
- Short ground processing time
- Long loiter capability in lunar orbit
- **Need to asses vehicle health and status rapidly and accurately on the ground and during quiescent periods**
- Design for ISHM

Robotic Space Exploration



- **Augment traditional fault protection/redundancy management/ FDIR with ISHM**
- Real-time HM of science payloads and engineering systems including anomaly detection, root cause ID, prognostics, and recovery
- Ground systems for real-time and system lifecycle health management

International Space Station & Space Shuttle



- **Prognostics** for ISS subsystems (power, GN&C)
- **Augment mission control capabilities (data analysis tools, advanced caution and warning)**
- Retrofit sensors (e.g., Shuttle wing leading edge impact detection)

Irem Y. Tumer
irem.tumer@oregonstate.edu

Complex System Design

Summary of Research Efforts

- Methods and tools to support engineering analysis and decision-making during *early conceptual design stages*
  - Functional analysis and modeling of conceptual designs for early fault analysis
  - Function based model selection for systems engineering
  - Functional failure identification and propagation analysis
  - Modeling, analysis, and optimization of ISHM Systems
  - Function based analysis of critical events
  - Quantitative risk assessment during conceptual design
  - Cost-benefit analysis of ISHM systems
  - Decision support and uncertainty modeling for design teams during trade studies
  - Risk assessment during early design

Function-Based Modeling and Failure Analysis

Objectives

- Improve the design process through early failure analysis based on functional models
- Produce a model-based early design tool to design safeguards against functional failures in vehicle design

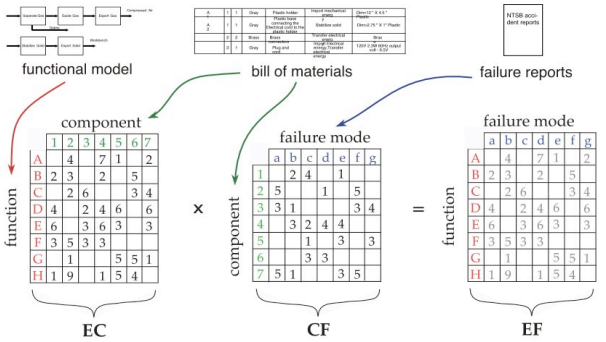
Benefits

- Reduced redesign costs through early failure identification and avoidance
- Improved mission risk assessment through identification of "unknown unknowns"
- Effective reuse of lessons-learned and commonalities across systems and domains
- Availability of generic and reusable function models and failure databases

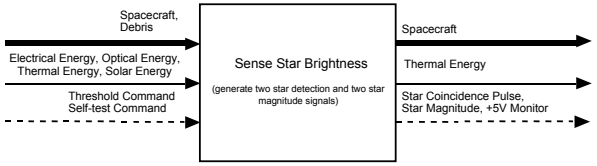
Approach

- Build generic and reusable functional models of existing subsystems using standardized function taxonomy (developed at UMR by Prof. Rob Stone)
- Generate failure lists for existing subsystems (failure reports, FMEAs) and build standardized failure taxonomy
- Map failures to functional models to create function-failure knowledge bases (resuable and generic)
- Develop software tools for use by design engineers
- Validate utility in actual design scenario

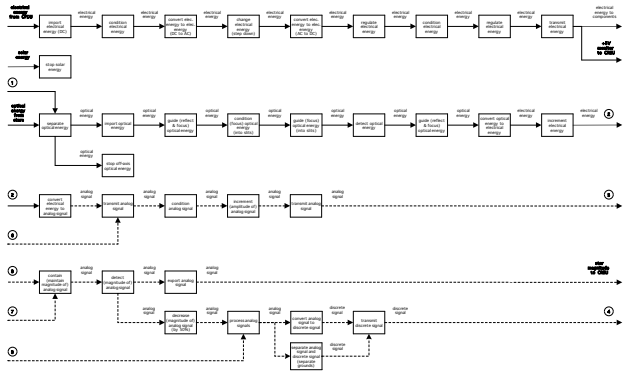
Approach:



Ex: Probe Cruise Stage: Star Scanner Assembly black box functional model is the highest level description of system:



Star Scanner functional model at the secondary/tertiary level of functional detail comprises approximately 60 identified functions:



Irem Y. Tumer
irem.tumer@oregonstate.edu

Function-Based Model Selection

Systems Engineering

Objectives

- Develop a function-based framework for the mathematical modeling process during the early stages of design

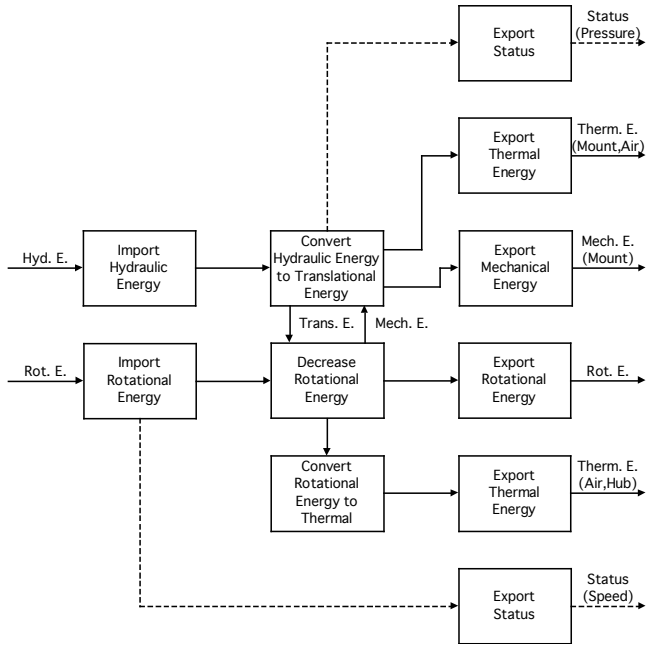
Benefits

- Provides a framework for identifying and associating various mathematical models of a system throughout the design process
- Enables quantitative evaluation of concepts very early in design process
- Promotes storage and re-use of mathematical models
- Represents the effect of assumptions and design choices on the functionality of a system

Methods

- During System Planning:
  - •Modeling Desired Functionality
  - •Generating System-level Requirements
  - •Modeling for Requirements Generation
- During Conceptual Design:
  - •Refining Functionality
  - •Modeling for Component Selection
  - •Component Selection
- During Embodiment Design:
  - •Auxiliary Function Identification
  - •Sub-system Functional Modeling
  - •Sub-system Level Requirements Identification
  - •Detailed System Modeling and Validation

Ex: Hydraulic Braking System



Function	Input	Output	Model Type
Import Hydraulic Energy	Flow, Pressure	Flow, Pressure	Closed-form Eqs.
Convert Hyd. E. to Trans. E.	Flow, Pressure	Displacement, Force	Closed-form Eqs.
Decrease Rot. E.	Force, Angular Speed, Moment	Angular Acceleration	ODE
Convert Rot. E. to Therm. E.	Angular Speed, Moment	Energy Magnitude	Closed-form Eqs.

Flow	Requirement
Rot. E.	Based on a 1500kg mass stopping from 30m/s, the braking system shall be able to handle a 675kJ energy input. The system shall be designed to stand a 180 rad/s max rotational speed and a maximum input moment of 13.5kN-m.
Hyd. E.	The maximum pressure input to the system shall be 10MPa.
Rot. E.	The output rotational energy output of the system shall be 0kJ.
Therm. E.	Based on a 2s stopping distance, the heat dissipation of the system shall be at least 337.5kW. The maximum temperature the system should reach is 150C.

Irem Y. Tumer
irem.tumer@oregonstate.edu

Simulation-Based Functional Failure Identification and Propagation Analysis

Objectives

- Develop a formal framework for design teams to evaluate and assess functional failures of complex systems during conceptual design

Benefits

- Systematic exploration of what-if scenarios to identify risks and vulnerabilities of spacecraft systems early in the design process
- Analysis of functional failures and fault propagation at a highly abstract system configuration level before any potentially high-cost design commitments are made
- Support of decision making through functional failure analysis to guide designers to *design out* failure through the exploration of design alternatives

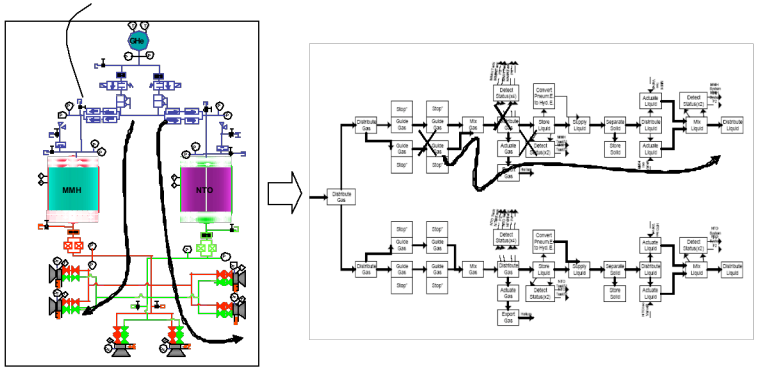
Approach

- Build generic and reusable system models using an interrelated set of graphs representing function, configuration, and behavior.
- Model behavior using a component-based approach using high-level, qualitative models of system components at various discrete nominal and faulty modes
- Develop a graph-based environment to capture and simulate overall system behavior under critical conditions
- Build a reasoner that translates the physical state of the system into functional failures
- Validate the framework in an actual design scenario

Example: Reaction Control System (RCS) Conceptual Design

Objective: Explore what-if scenarios:
What are the effects of component failures on overall system functionality?

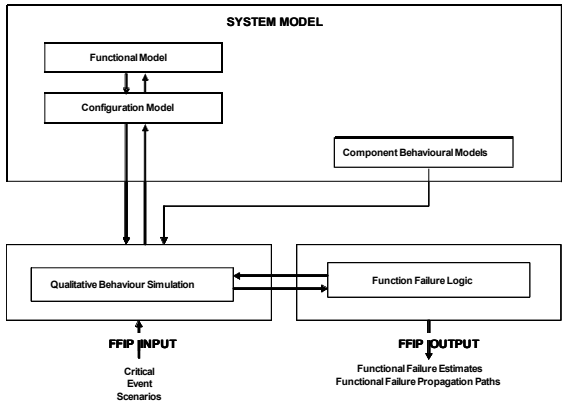
The FFIP framework identifies potential functional failures and their propagation under off -nominal conditions using behavioral analysis.



System Configuration: Conceptual Schematic

System Function: Functional Model

Functional Failure Identification and Propagation (FFIP) Architecture



Irem Y. Tumer
irem.tumer@oregonstate.edu

Function-Based Analysis of Critical Events

Objectives

- Establish a standard framework for identifying and modeling critical mission events
- Establish a method for identifying the information required to ensure that these critical events occur as planned
- Provide a means to determine Health Management needs, sensor locations, etc. during early design phase
- Assist the identification of requirements for critical events during the design of space flight systems

Benefits

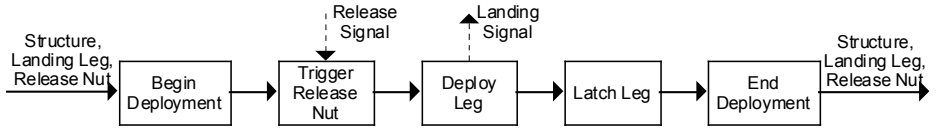
- Standardized function-based modeling framework
- Development of event models and functional models very early in the design of systems
- Identification of critical events and important functionality from these models
- Requirements identification based on functional and event models

Methods

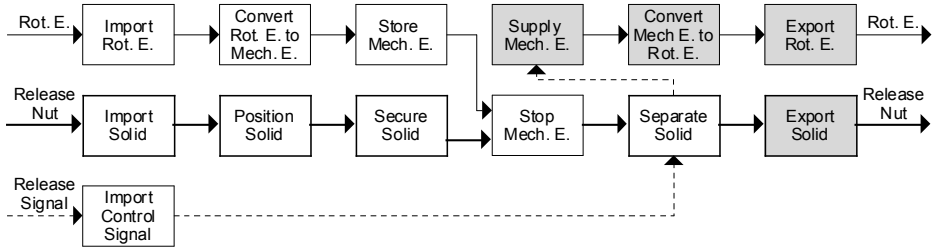
- Event Models for Systems
  - •Black Box
  - •Detailed
- Functional Models During Events
  - •Black Box
  - •Detailed
- Function-based Requirements Identification

Approach:

Ex: Mars Polar Lander Landing Leg: Event Model During Landing Leg Deployment



Functional Model During Landing Leg Deployment



Requirements Identified from Functional and Event Models

Flow Type	Flow	Requirement
Solid Input	Release Nut	The release nut must be properly positioned and secured before the release event can occur
Control Signal Input	Release Signal	The Release Signal will initiate the Trigger release Nut event
Solid Output	Release Nut	At the completion of the event, the Release Nut will be separated from the landing leg
Signal Output	Separation	After completion of the event, the subsequent event will be initiated without a formal signal

Irem Y. Tumer
irem.tumer@oregonstate.edu

Model-Based Design & Analysis of ISHM Systems

Objectives

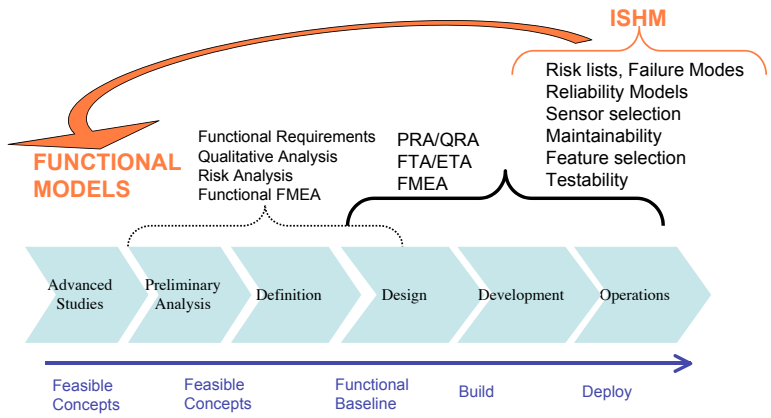
- Concurrent design of ISHM systems with vehicle systems to ensure reliable operation and robust ISHM
- Model-based optimization of ISHM design and technology selection to reduce risks and increase robustness

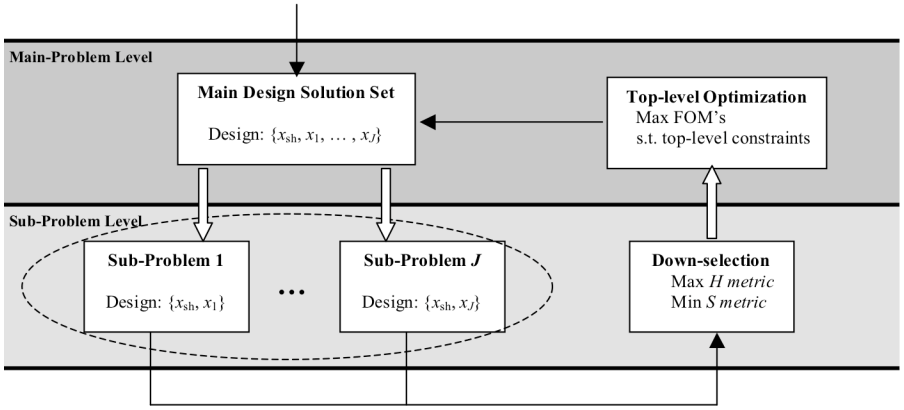
Benefits

- Identification of issues, costs, and constraints for ISHM design to reduce cost and increase reliability of ISHM and optimize mitigation strategies
- Streamlining the design process to decide when and how to incorporate ISHM into system design, and how to balance between cost, performance, safety and reliability
- Provide subsystem designers with insight into system level effects of design changes.

Approach

- Formulate ISHM design as optimization problem
- Leverage research & tools for function-based design methods, risk analysis, and design optimization to incorporate ISHM design into system design practices
- Develop ISHM software design environment using ISHM optimization algorithms
- Implement and validate inclusion of ISHM chair in concurrent design teams (e.g., Team-X)



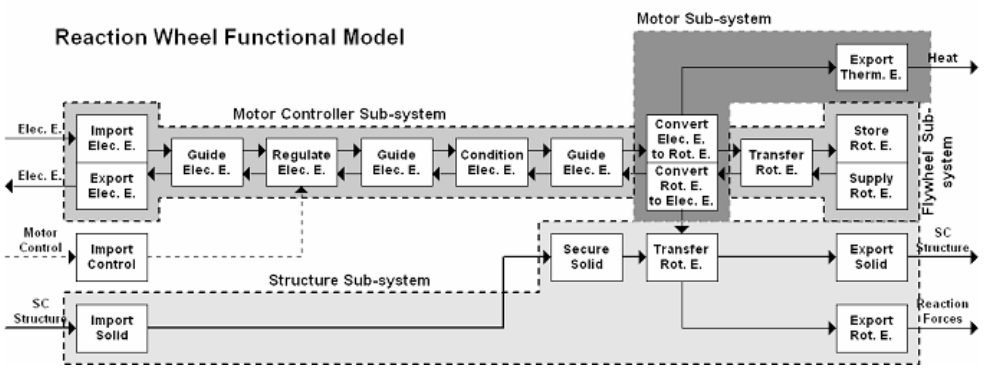


Irem Y. Tumer
irem.tumer@oregonstate.edu

Risk Quantification During Concurrent Design

Objectives

- Enable rapid system level risk trade studies for concurrent engineering design
- Develop a quantitative risk-analysis methodology that can be used in the concurrent design environment
- Provide a real-time (dynamic) resource allocation vector that guides the design process to minimize risks and uncertainty based on both failure data and designers' inputs

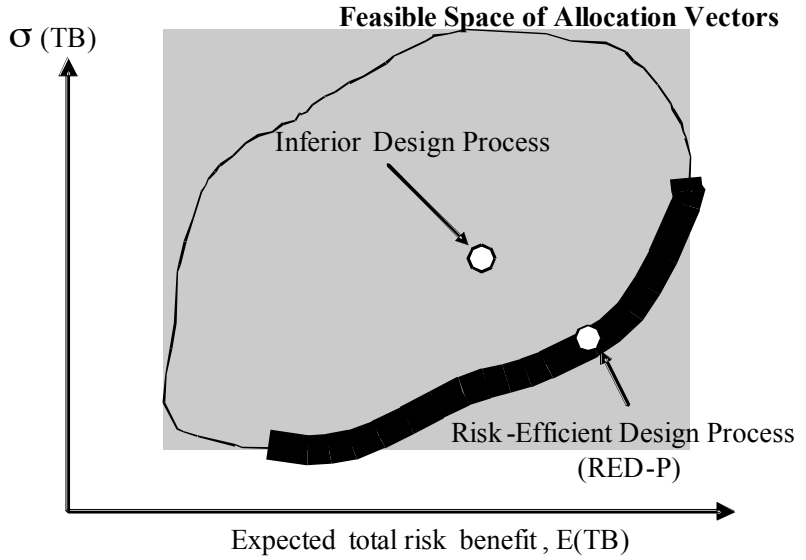


Benefits

- Improved resource management and reduced design costs through early identification of risks & uncertainties
- Use common basis for trading risk with other system and programmatic resources
- Increased reliability and effectiveness of mission systems

Approach

- Develop functional model
- Collect failure rates and pairwise correlations
- Model design as a stochastic process
- Formulate as a 2-objective optimization problem
- Obtain the optimal resource allocation vector in real-time, as the design evolves



Irem Y. Tumer
irem.tumer@oregonstate.edu

Cost-Benefit Analysis for ISHM Design

Objective:

- *Create a cost-benefit analysis framework for ISHM that enables:*
  - *Optimal design of ISHM (sensor placements etc.)*
  - *Tradeoff analysis (does the benefit justify the cost?)*

Approach:

- Maximize "Profit"!

$$\Pi = A \cdot R - C = \prod_{i=1}^{N+M} A_i \cdot R - \sum_{i=1}^{N} (C_R + C_D)_i$$

where:

- P is Profit
- *A* is Availability, a function of System Reliability, Inspection Interval, and Repair Rate.
- *N* is number of System Functions.
- *M* is the number of ISHM Sensor Functions utilized.
- *R* is Revenue/Unit of Availability in USD.
- Cost of Risk: quantifies financial risk in USD.
- Cost of Detection: quantifies cost of detection of a fault in USD.

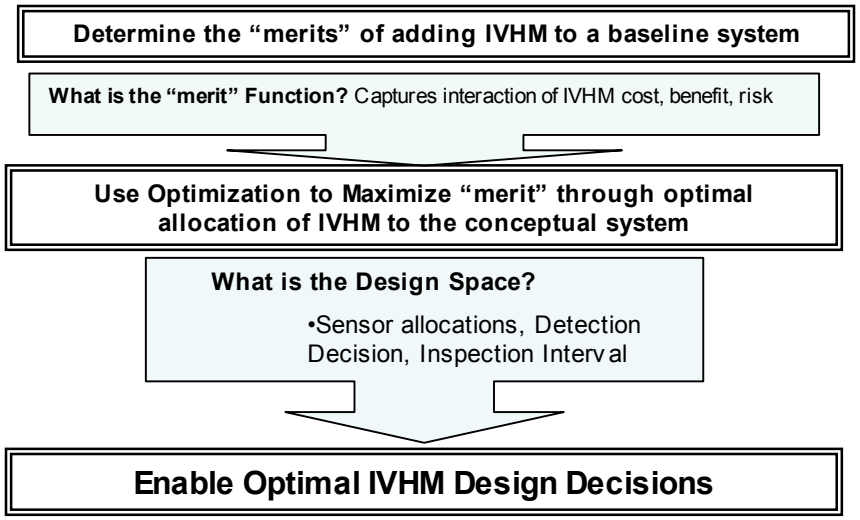
Irem Y. Tumer
irem.tumer@oregonstate.edu

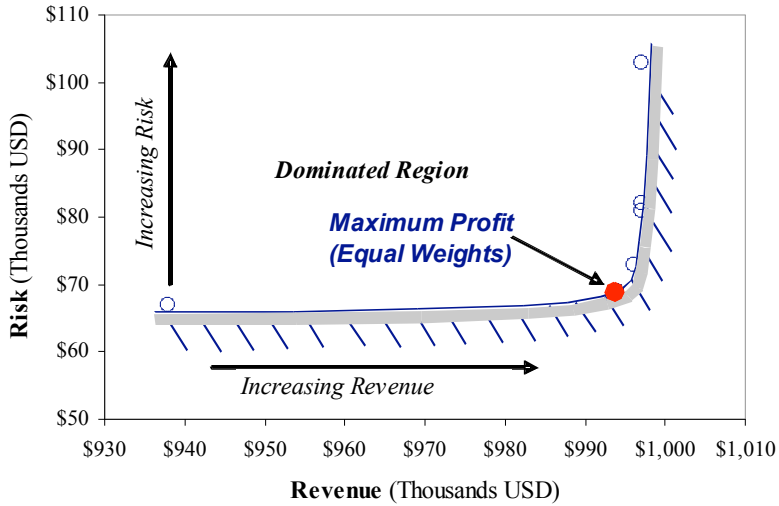
Cost-Benefit Analysis Process

Approach:

1. Develop models to measure the impact of various IVHM architectures (i.e. sensor placements, data fusion algorithms, fault detection and isolation methodologies) on the safety, reliability, and availability of the vehicle.
2. Once the impact of various IVHM architectures on the vehicle are measured, tradeoffs are formulated as a multiobjective multidisciplinary optimization problem.
3. We can then create a decision support system for the designers to handle IVHM tradeoffs at the early stages of designing a system.

Since the Profit function is impacted by a combination of *revenue* and cost of *risk*, a Pareto Frontier can be created. The frontier demonstrates the solution for different trade-offs.





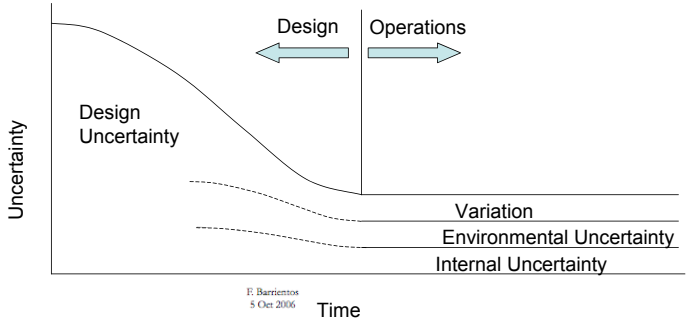
Irem Y. Tumer
irem.tumer@oregonstate.edu

Decision Support for Engineering Design Teams

Uncertainty capture, modeling, & management

Objectives

- Facilitate collaborative decision-making and concept evaluation in concurrent engineering design teams
- Characterize uncertainty and risk in decisions from initial design stages
- Develop decision management tool for integration into collaborative design and concurrent engineering environments

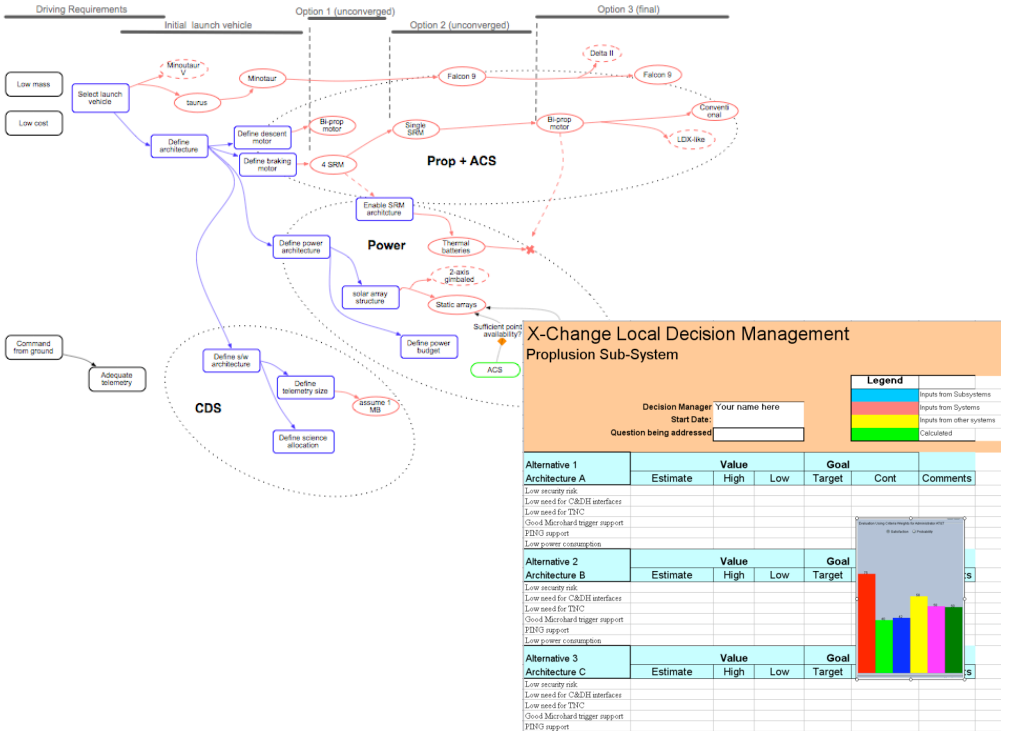


Benefits

- More robust designs starting from conceptual design stage
- Reduced design costs
- Modeling important decisions points in highly-concurrent engineering design teams
- Incorporating tools and methods into fluid and dynamic design environment

Approach

- Understand uncertain decision-making in real design teams
- Develop framework to map design decision-making to decision-theoretic models
- Validate method and tool with a real engineering teams



Irem Y. Tumer
irem.tumer@oregonstate.edu

Risk in Early Design (RED) Methodology

Objectives

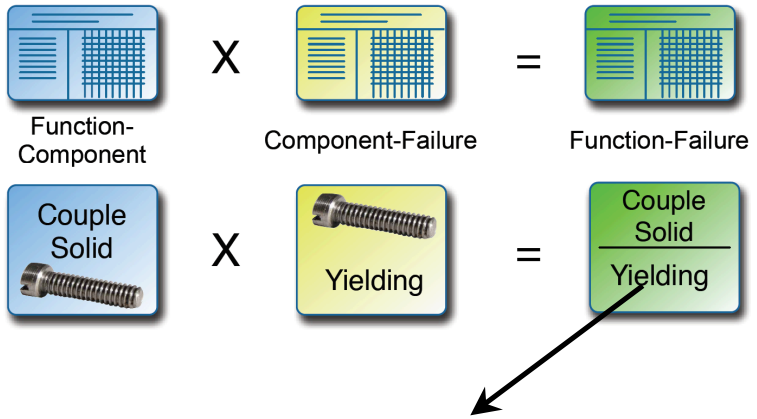
- Identify and assess risks during conceptual product design
- Effectively communicate risks

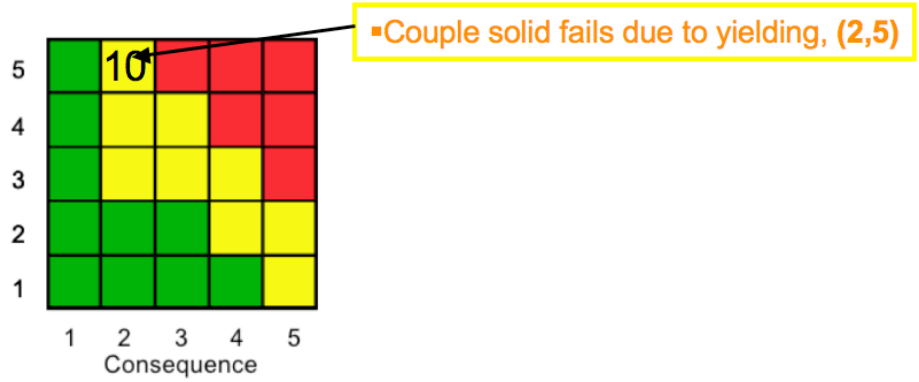
Benefits

- Improved Reliability
- Decreased cost associated with design changes

Methods

- FMEA
  - RED can id system functions failure modes, occurrence, and severity
- Fault Tree Analysis
  - RED can id at risk functions and potential failure paths from functional models
- Event Tree Analysis
  - RED can id sequences of functions and subsystems at risk from initiating events





Irem Y. Tumer
irem.tumer@oregonstate.edu