Design for Supportability

Includes

Integrated Vehicle Health Management
Integrated System Health Management

Mike Battaglia
202-358-4658

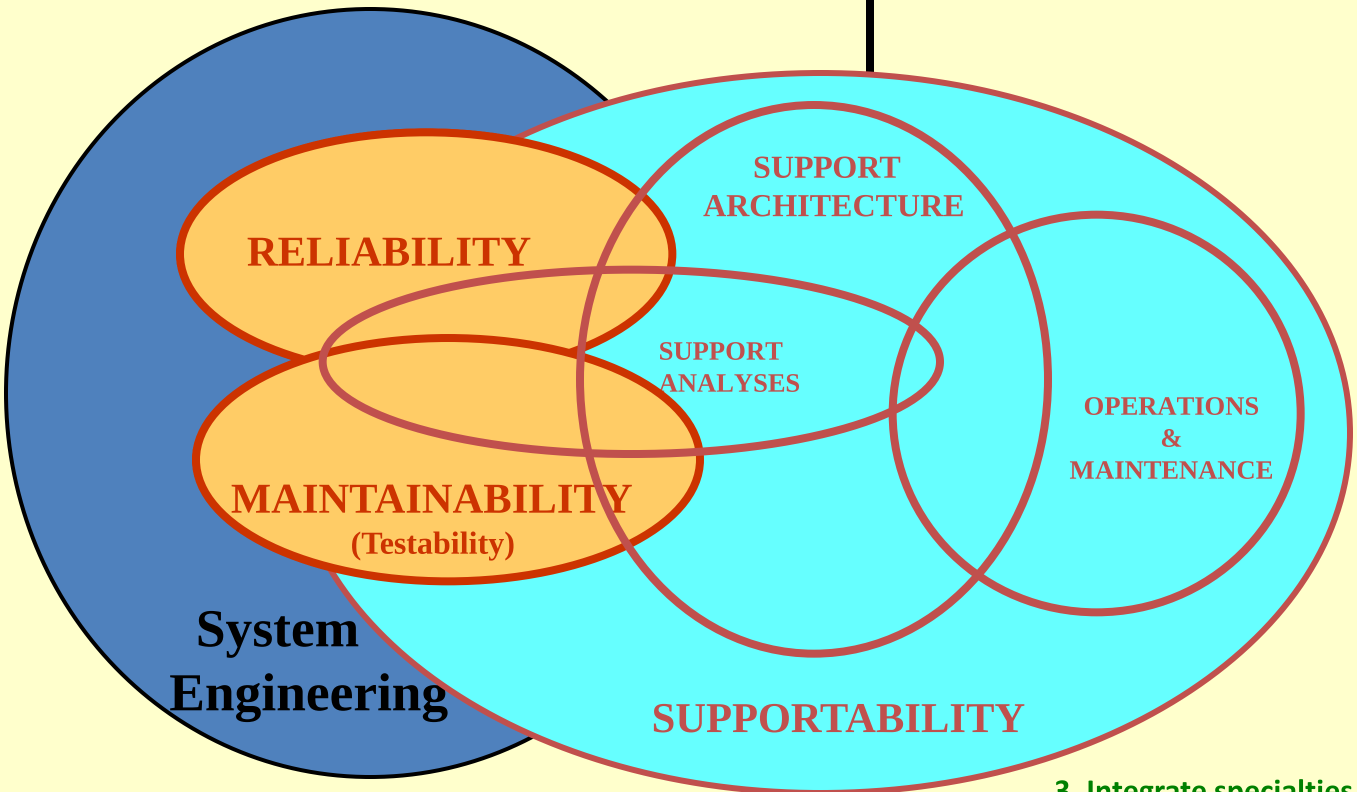
From the President's Talking Points at KSC April 15, 2010

- Make strategic investments to develop critical knowledge, technologies, and capabilities to expand long-duration human exploration into deep space in a more efficient and safe manner, thus getting us to more destinations in deep space sooner.

- Initiate a vigorous new technology development and test program to increase the capabilities and reduce the cost of future exploration activities.

Supportability

System Engineering's Integration Role



1. Translate operational needs into verifiable system performance parameters.

2. Integrate & optimize technical parameters and ensure compatibility of physical, functional and program interfaces .

3. Integrate specialties into total design process (R&M, Logistics Support, Safety, Producibility, Human Factors, etc.)

Design & Development Phase

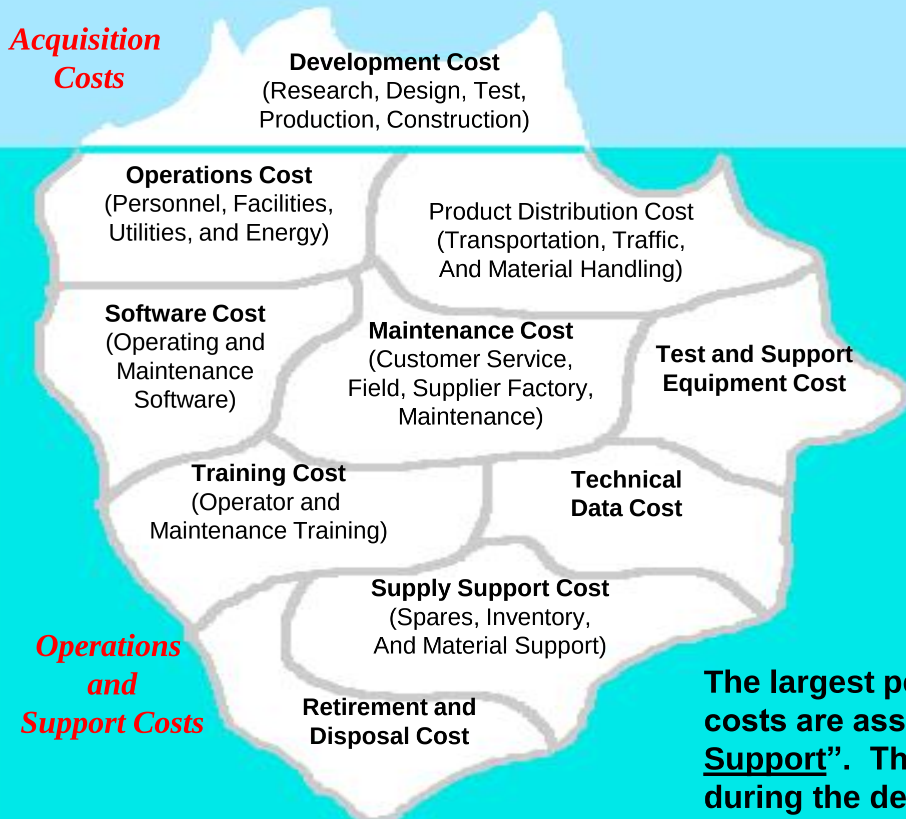
(Product Effectiveness)

Operations and Support Phase

(Support Efficiency)

Program Life Cycle

Supportability Considers Total System "Cost of Ownership"



A Program focusing on "Product Inherent Design" only during the Development phases

Approximately 70% of a project's life cycle costs (LCC) are determined at the concept phase

The largest percentage of System ownership costs are associated with "Operations and Support". These costs are often overlooked during the development phase, where focus is often on the cost of acquisition only.

Supportability Design Drivers

- Reliability
- Testability
- Diagnostics
- Prognostics
- Maintainability
- Commonality/interchangeability
- Affordability
- Producibility
- Sustainability
- Dependability
- Interoperability
- Accessibility
- Sparing / resupply
- Verification / validation
- Transportability
- Disposability
- Life Cycle Cost

What is Integrated Vehicle/System Health Management?

Vehicle/System Health Management is a disciplined process for designing, assessing and maintaining the health of systems and machines…

and draws upon:

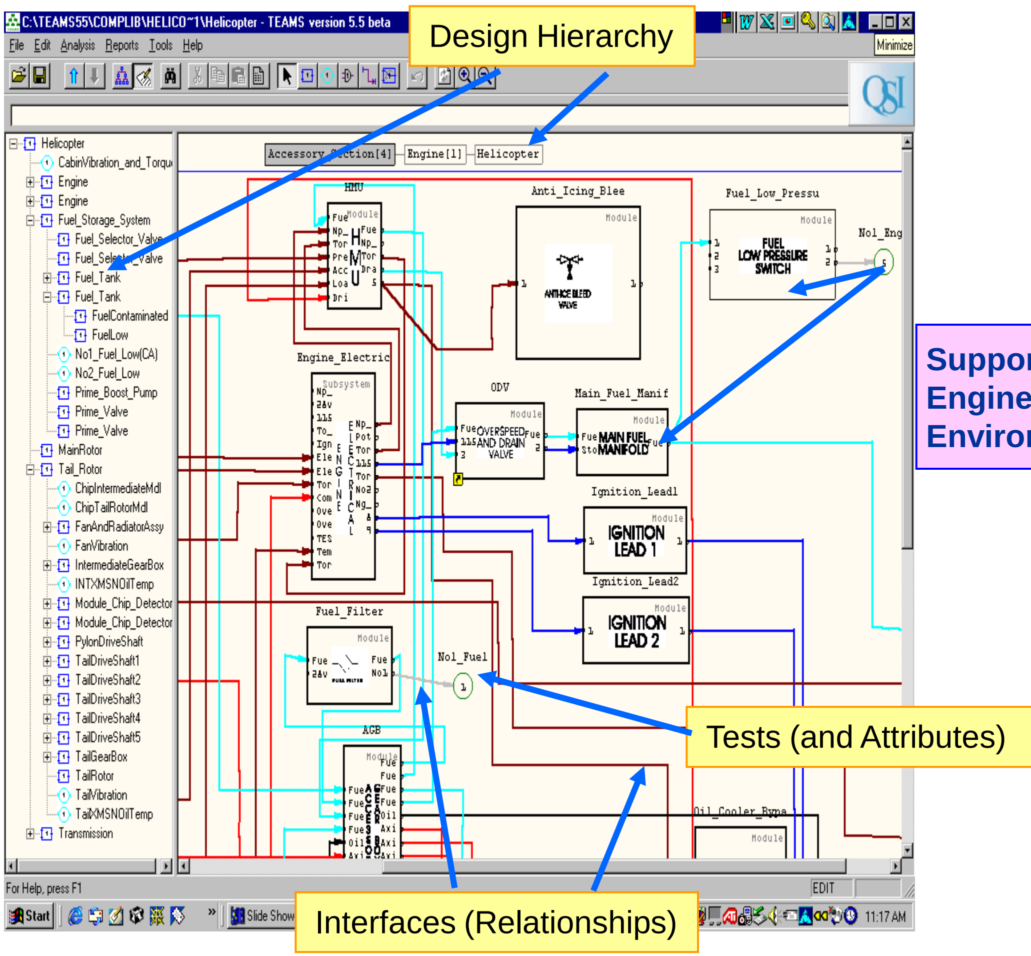
- System architecture, engineering & design knowledge capture and management
- Classical engineering design practices, such as, the use of sensors, redundancy management, diagnostics and prognostics, risk assessment, fault tree analysis, testability analysis, maintainability analysis and human factors.
- Safety assurance
- Verification/validation

What Does IVHM/ISHM Design Directly Influence?

- Availability and Reliability of systems
- Safety and Risk design
- Maintenance man-hours
  - crew time for maintenance
  - maintenance training
  - maintenance documentation
- Mission support requirements and costs (spares, test equipment, levels of maintenance)
- Verification/validation of the above to meet mission requirements

Failure Space Modeling &Analysis

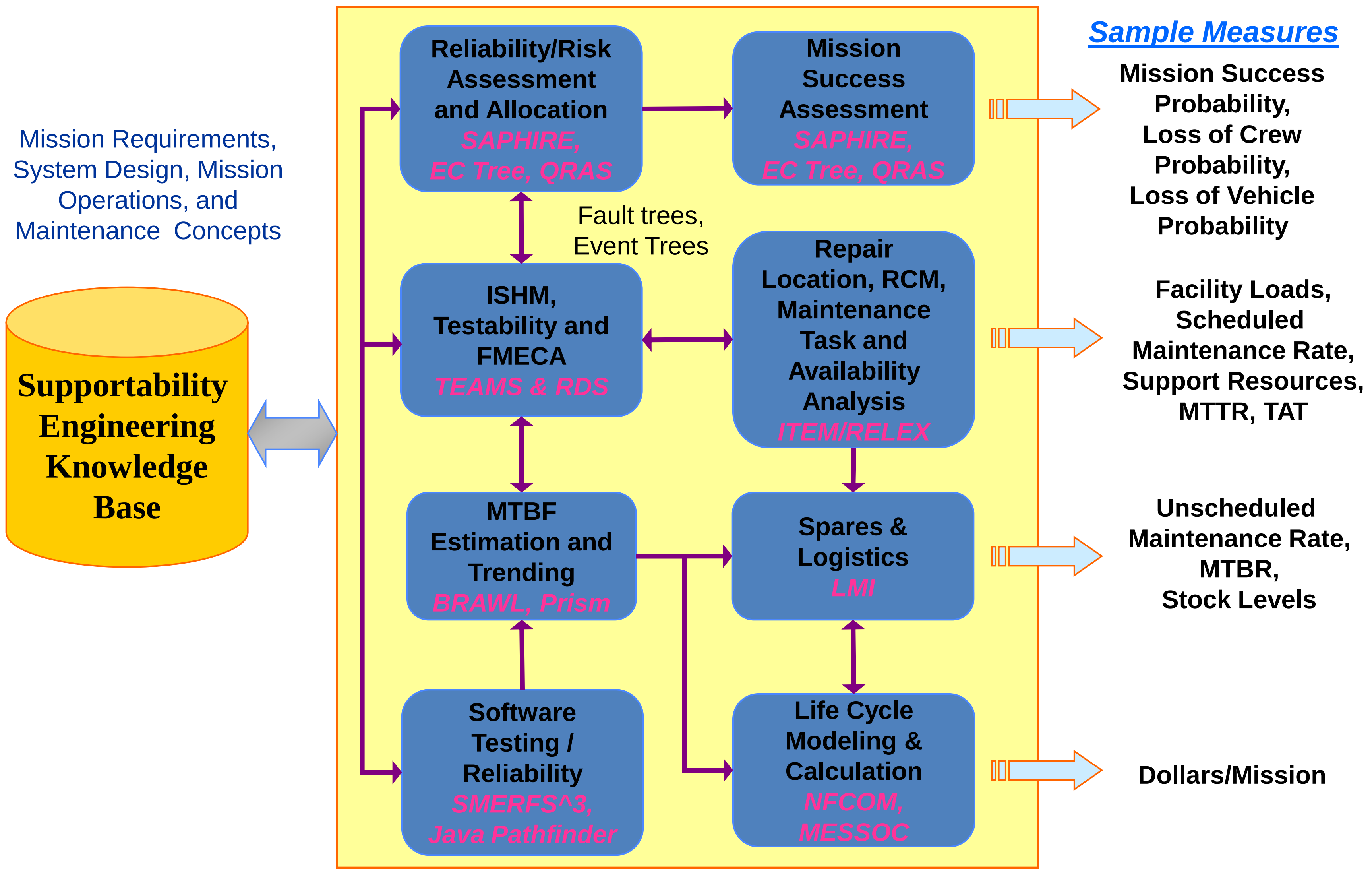
Failure Effects Model

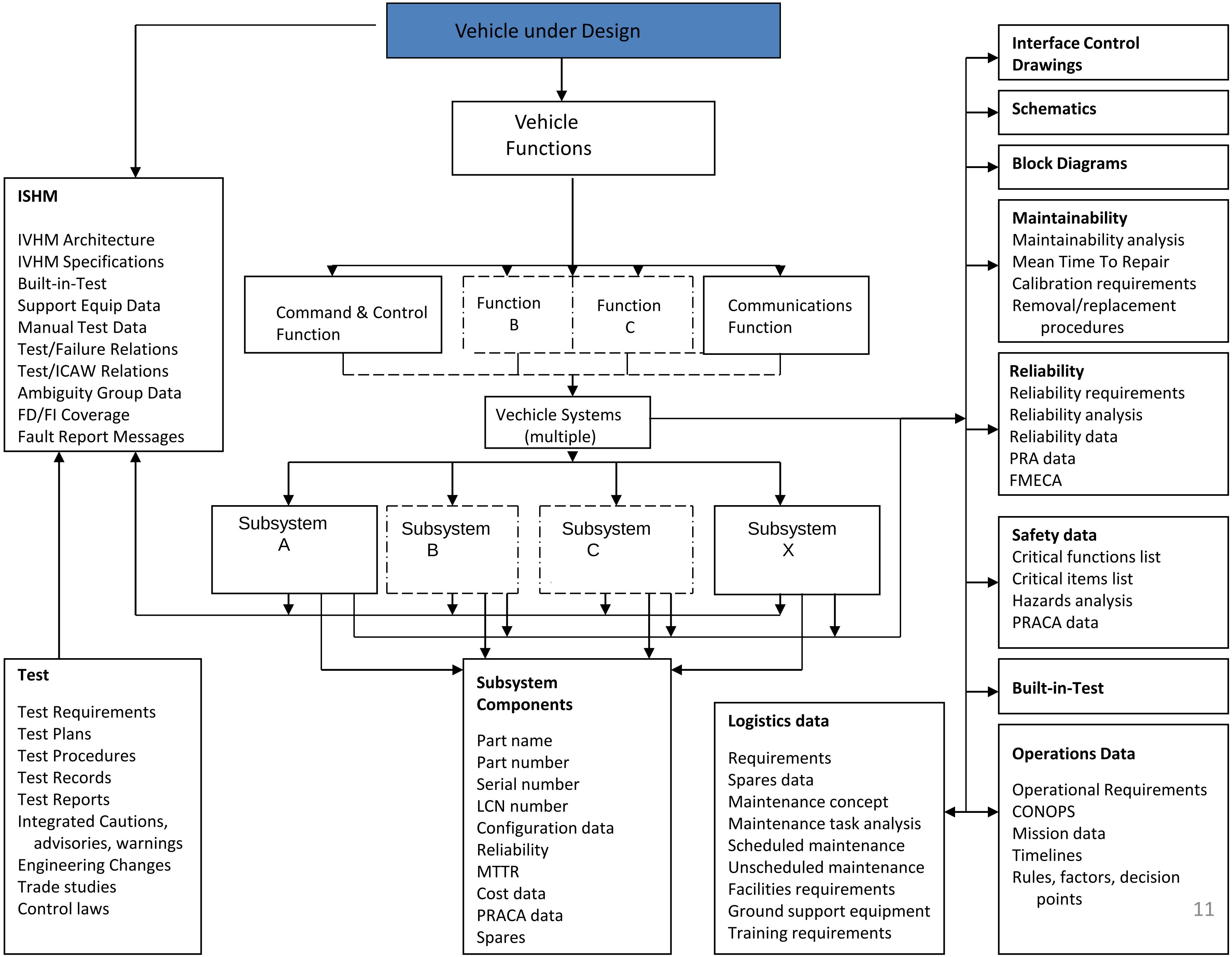


Supportability Engineering Environment

- Fault Detection/Isolation Coverage (%FD/FI)
- Optimal Sensor Allocation for FD/FI
- Ambiguity Groups and Frequency
- Time to Criticality
- Latency
- Criticality of All Failure Modes
- Safety Critical Coverage
- Mission Critical Coverage
- Weight of HM (Health Management) System
- Cost of HM System
- Volume of HM System
- Memory Requirements for HM
- Processing Requirements (CPU Usage)
- Near Optimal Diagnostic Strategy (Cost vs. Time)
- Maintenance Concept (Series vs. Block Replacement)
- Time to Isolate, Time to Repair (Mean, Min, Max, Av..)
- Predicted False Alarm Rate
- Vehicle Level FMECA - Comprehensive - Across all Systems
- Mission Reliability
- Appropriate ICAW (Indications, Cautions, Advisories, and Warnings)
- Appropriate Procedure to Mitigate and/or Repair

Supportability Engineering Environment Tool Interactions





Vehicle under Design
Vehicle Functions
ISHM
IVHM Architecture
IVHM Specifications
Built-in-Test
Support Equip Data
Manual Test Data
Test/Failure Relations
Test/ICAW Relations
Ambiguity Group Data
FD/FI Coverage
Fault Report Messages
Command & Control Function
Function B
Function C
Communications Function
Vechicle Systems (multiple)
Subsystem A
Subsystem B
Subsystem C
Subsystem X
Test
Test Requirements
Test Plans
Test Procedures
Test Records
Test Reports
Integrated Cautions, advisories, warnings
Engineering Changes
Trade studies
Control laws
Subsystem Components
Part name
Part number
Serial number
LCN number
Configuration data
Reliability
MTTR
Cost data
PRACA data
Spares
Logistics data
Requirements
Spares data
Maintenance concept
Maintenance task analysis
Scheduled maintenance
Unscheduled maintenance
Facilities requirements
Ground support equipment
Training requirements
Interface Control Drawings
Schematics
Block Diagrams
Maintainability
Maintainability analysis
Mean Time To Repair
Calibration requirements
Removal/replacement procedures
Reliability
Reliability requirements
Reliability analysis
Reliability data
PRA data
FMECA
Safety data
Critical functions list
Critical items list
Hazards analysis
PRACA data
Built-in-Test
Operations Data
Operational Requirements
CONOPS
Mission data
Timelines
Rules, factors, decision points

Questions to be addressed in Supportability Analysis & Design

Reliability & Maintainability

- How should reliability goals be allocated among systems?
- How should redundancy be managed?
- Do reliability predictions match the actuals?
- What is the optimal level of repair?
- Are replaceable units accessible and common parts interchangeable?

Safety

- What is the impact of a failure (criticality, **time to criticality**, risk, and hazard)?
- What is the likelihood of failure during a mission?
- How can the system be improved (hazard elimination, control)?

Questions to be addressed in Supportability Analysis & Design

Testability – IVHM/ ISHM/ Prognostics

- Are all potential failures (HW, SW, Human error) detectable & isolatable?
- Can detecting degradation or anomalies prevent failures or hazards and save support costs?
- Is the on-board and off-board allocation of the Health Management capability cost effective and operationally acceptable?
- How/where does a failure propagate?
- How could the system fail in every operational phase?
- Can multiple failures or battle damage take out critical functions?
- What are the consequences of failure across the integrated design?
- How is each failure detected and isolated by each test method?
- How are undetectable failures being addressed?
- How are fault isolation ambiguity groups being managed?
- How are safety related failures mitigated or eliminated?
- What is the impact of each failure on mission success?
- How can technicians troubleshoot problems in an expert manner, minimize downtime, and reduce maintenance manpower?

Questions to be addressed in Supportability Analysis & Design

Logistics and Spares Optimization

- What is the optimal level of spares for each line replaceable unit, taking into account failure effect, duty cycle, volume, weight and replacement opportunities?
- What is the impact of failures on Operations and Maintenance?
- What are the logistics impacts of failures (spares, procedures, training, etc.)?
- Where should spares be pre-positioned and which spares are needed to ensure the availability of critical functions?.
- How can commonality impact spares requirements and reduce acquisition and support costs?

Lifecycle Cost

- Are total ownership costs minimized while maintaining a specified availability and readiness level?

Benefits to Failure Space Modeling

- Provides a common graphical representation of the vehicle, system, sub-system, to the component level
- Integrates with existing engineering, safety, maintenance and logistical data bases
- Allows detailed design trade studies to provide optimal implementation of embedded diagnostics, fault tolerance, maintenance strategy (on-board/off-board), and logistical support
- Automates a number of analysis functions, thus
  - Reduces engineering work load
  - Provides insight into design decisions
  - Reduces conflicts, errors and omissions
  - Provides insights into operations costs and effectiveness during the design process – to realistically reflect what is to be expected in operations
- Seamless transition of diagnostic reasoners into the IVHM/ISHM (On Board/Off Board) solution ensures that fault detection, fault isolation, and failure mitigation perform as advertised

What is the status of Failure Space Modeling Today?

Current status:

- The fundamental algorithms exist today
- The methodology has been applied to NASA, DoD and commercial systems over the past 15 years

What's needed?

The automation and generation of Failure Space Modeling and Analysis.

This is a ***Game Changing Technology****, which can:*

- Save the government (DoD, NASA) billions of dollars in support costs.
- Reduce maintenance manpower
- Reduce design costs for diagnostics, safety and risk considerations
- Enable sound design trade-off considerations (diagnostics, spares, ambiguity groups, commonality, manpower requirements, etc.)
- Enable the contractor and government to V&V designs in meeting support requirements