Model-Driven Development of Integrated Support Architectures

Stan Ofsthun

Associate Technical Fellow

The Boeing Company

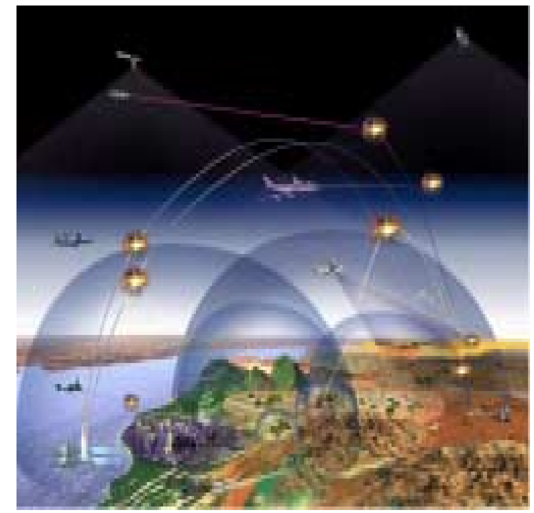
(314) 233-2300

October 13, 2004

Agenda

- Introduction
- Health Management Framework
  - Process Frameworks
  - Model-Based Design/Analysis Frameworks
  - Model-Based Software Frameworks
  - Model-Based Reasoning Frameworks
- Case Study
  - Engineering Models (Boeing ADVISE)
  - Run Time Diagnostic Models (ISIS GME/TFPG)
  - Practical Experiences and Issues
- Summary

The Need for Managing Complexity



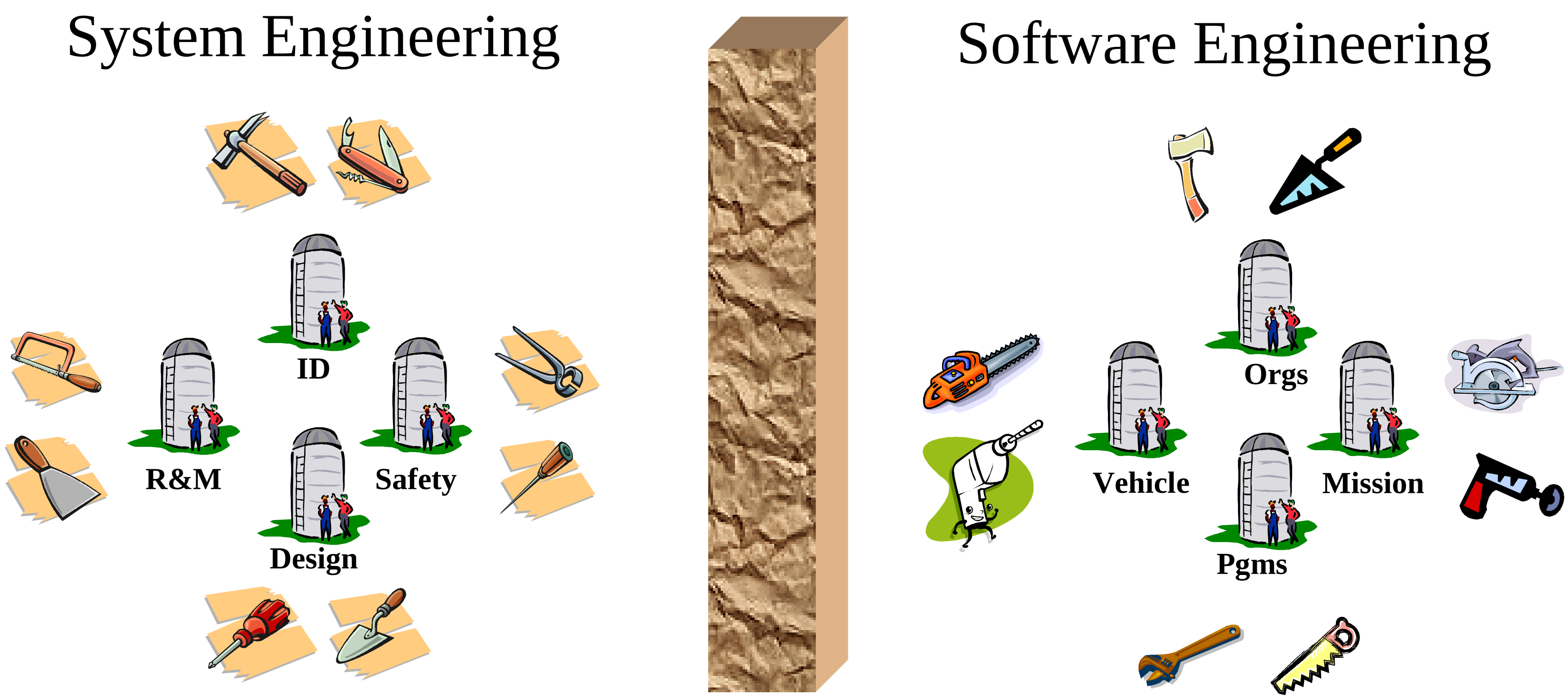
<u>**Built In Test**</u>
Component
Module
Subsystem

Integrated Diagnostics
Prognostics
Vehicle Health Management

Integrated SoS
Health Management

Given marginal historical diagnostic performance and increasing vehicle complexity/integration requirements, how do we produce a state of the art Health Management (HM) capability within the target support system?

Diagnostic Development Evolution



Traditional barriers have hindered the development of cost effective and robust Health Management (HM) applications…

Diagnostic Development Evolution

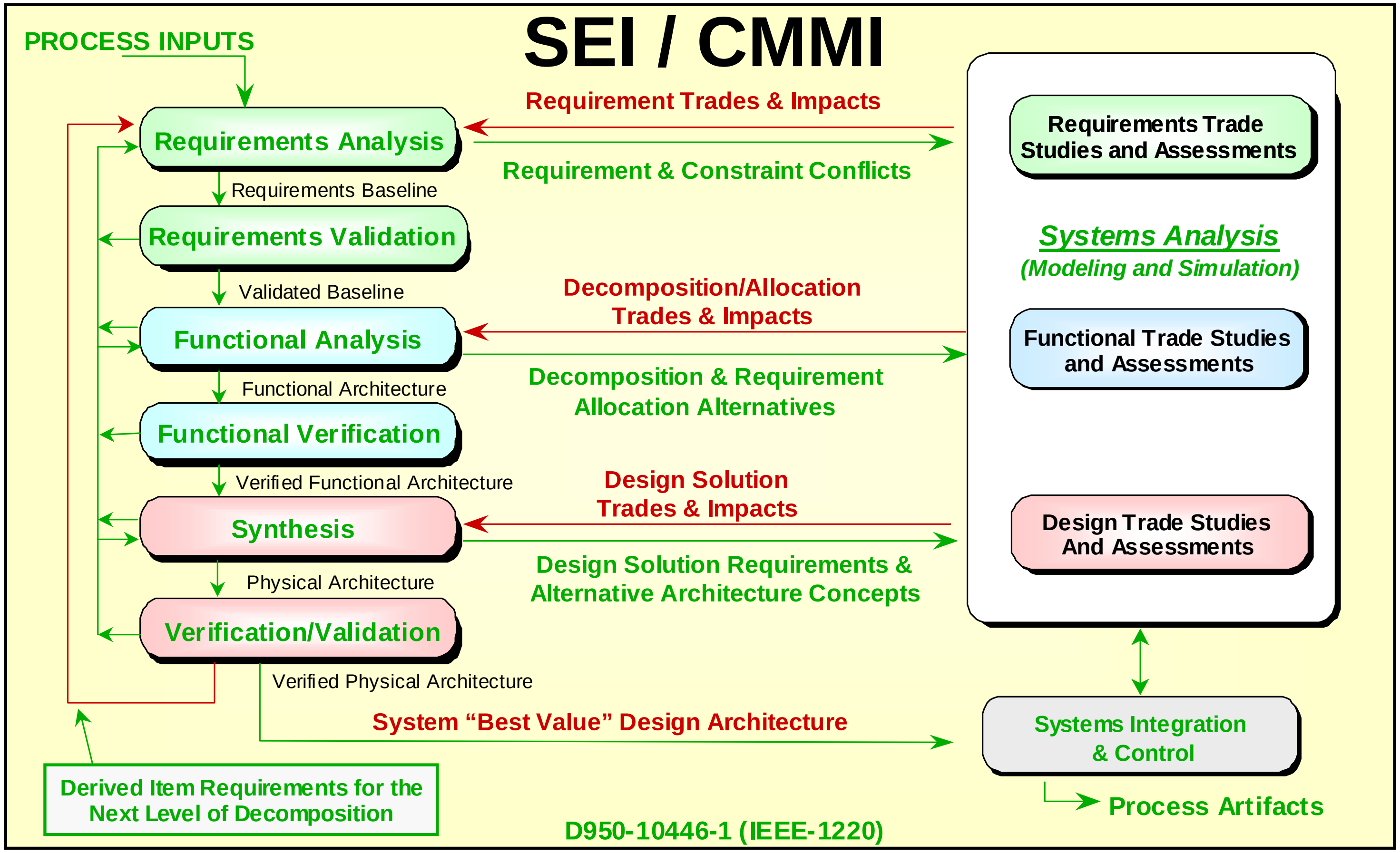
System Engineering

Software Engineering

CMMI SEI

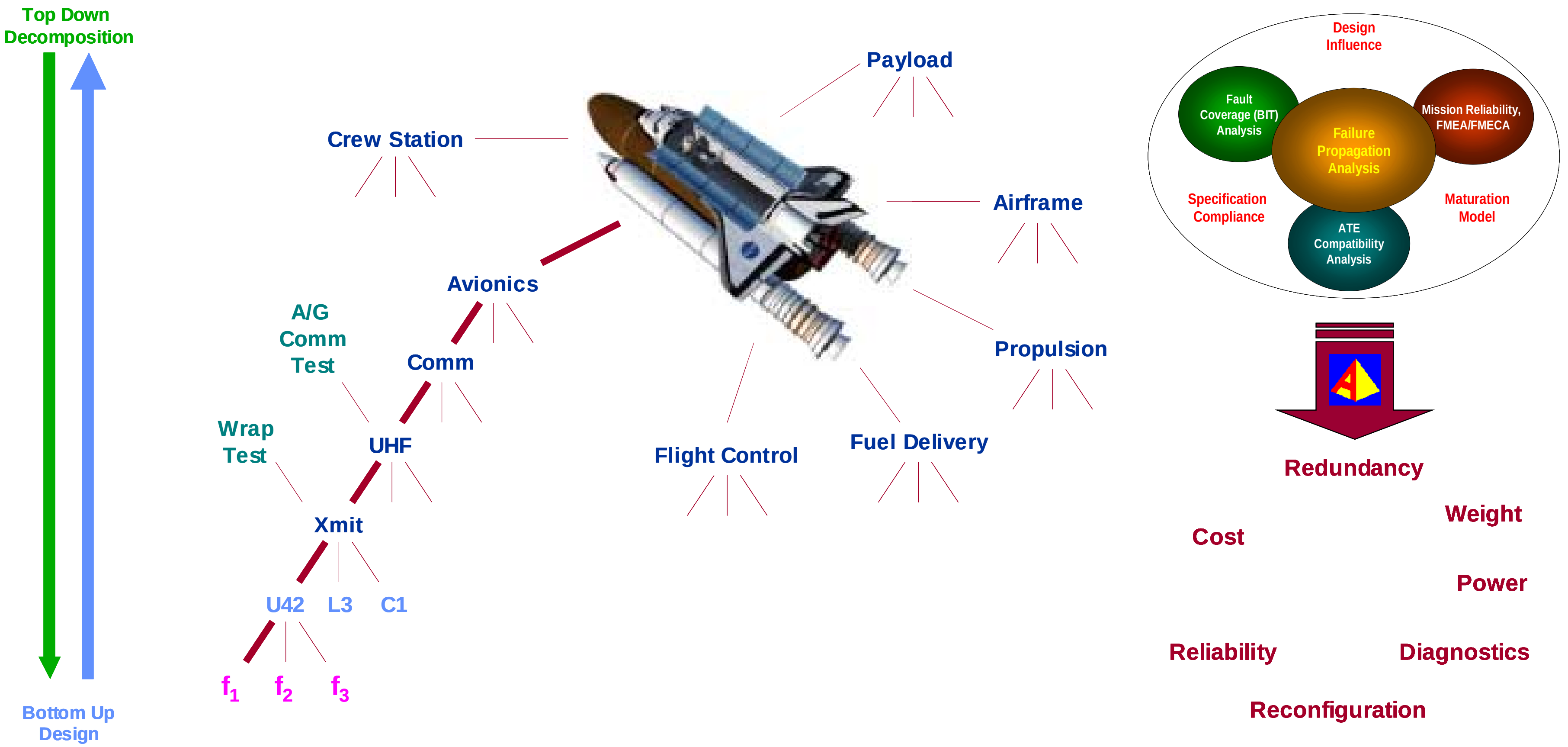
…which can be addressed by having a more integrated approach to Health Management (HM) processes and tools.

MBHM Process Frameworks



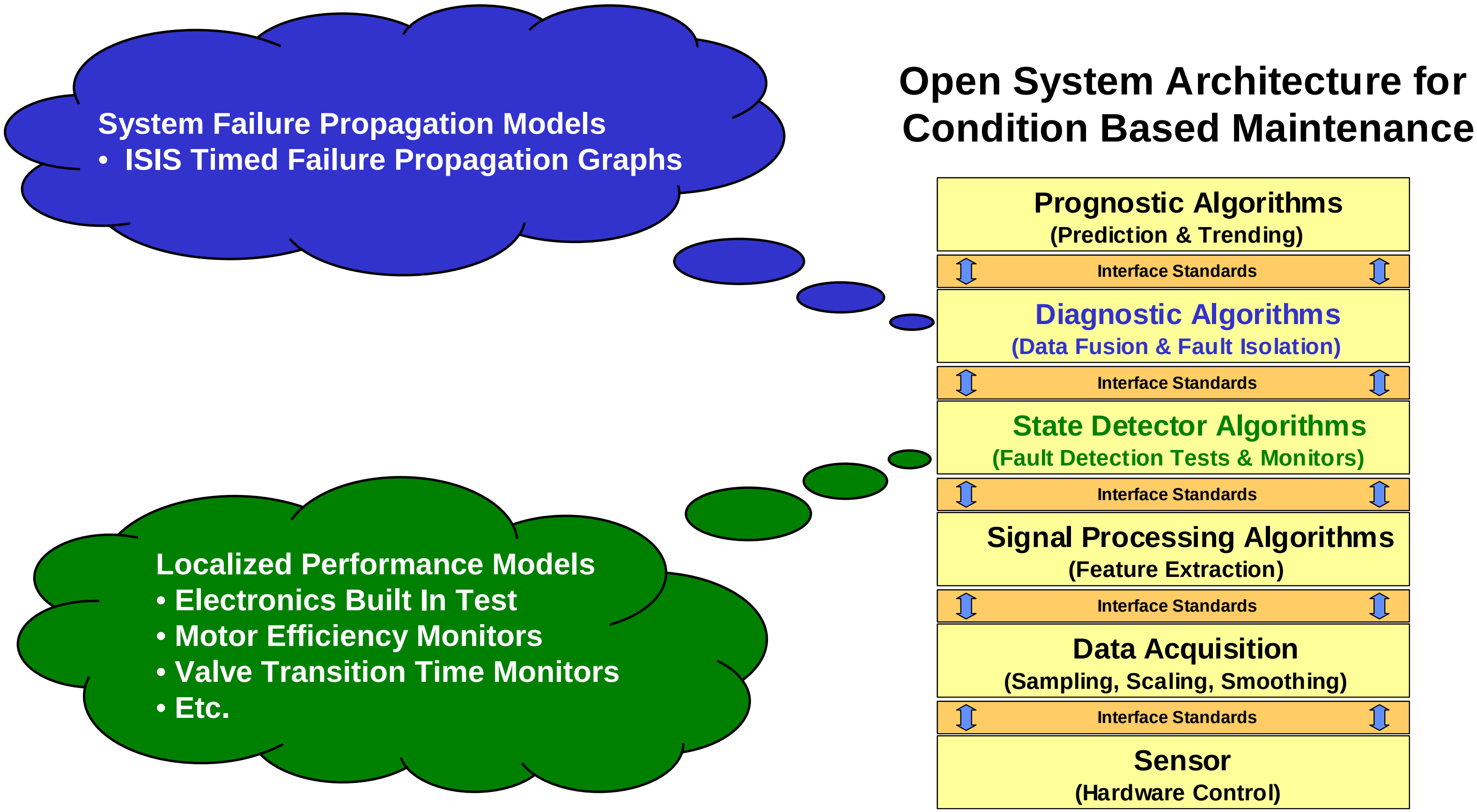
Because the HM function inherently touches every aspect of a system, decisions regarding HM requirements and design must be integral to the overall Systems Engineering (SE) process.

MBHM Design/Analysis Frameworks



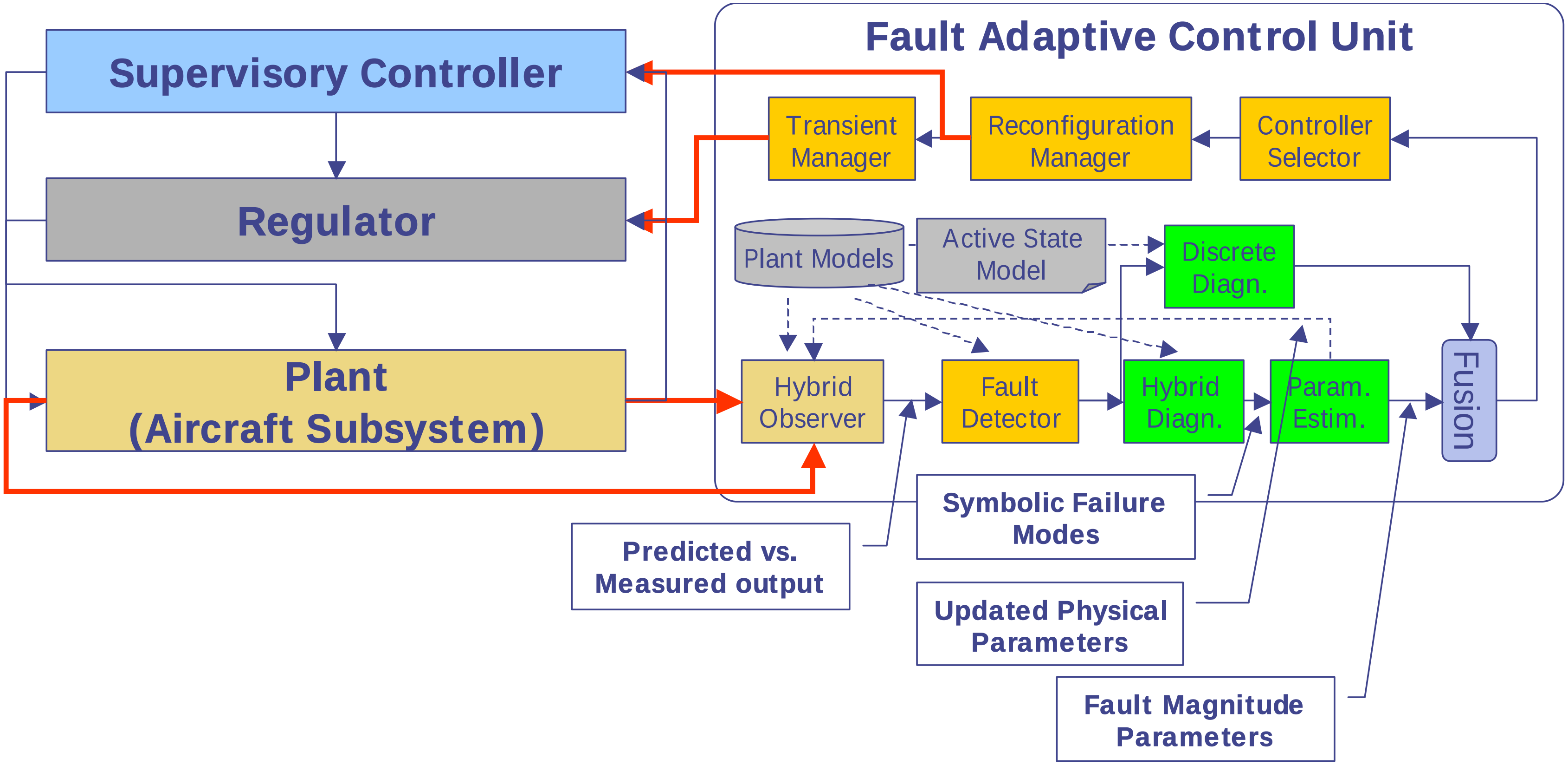
Model-Based design/analysis tools support the integration of HM and SE processes by providing an integrated assessment of many traditionally disparate aspects of failure propagation.

MBHM Software Frameworks



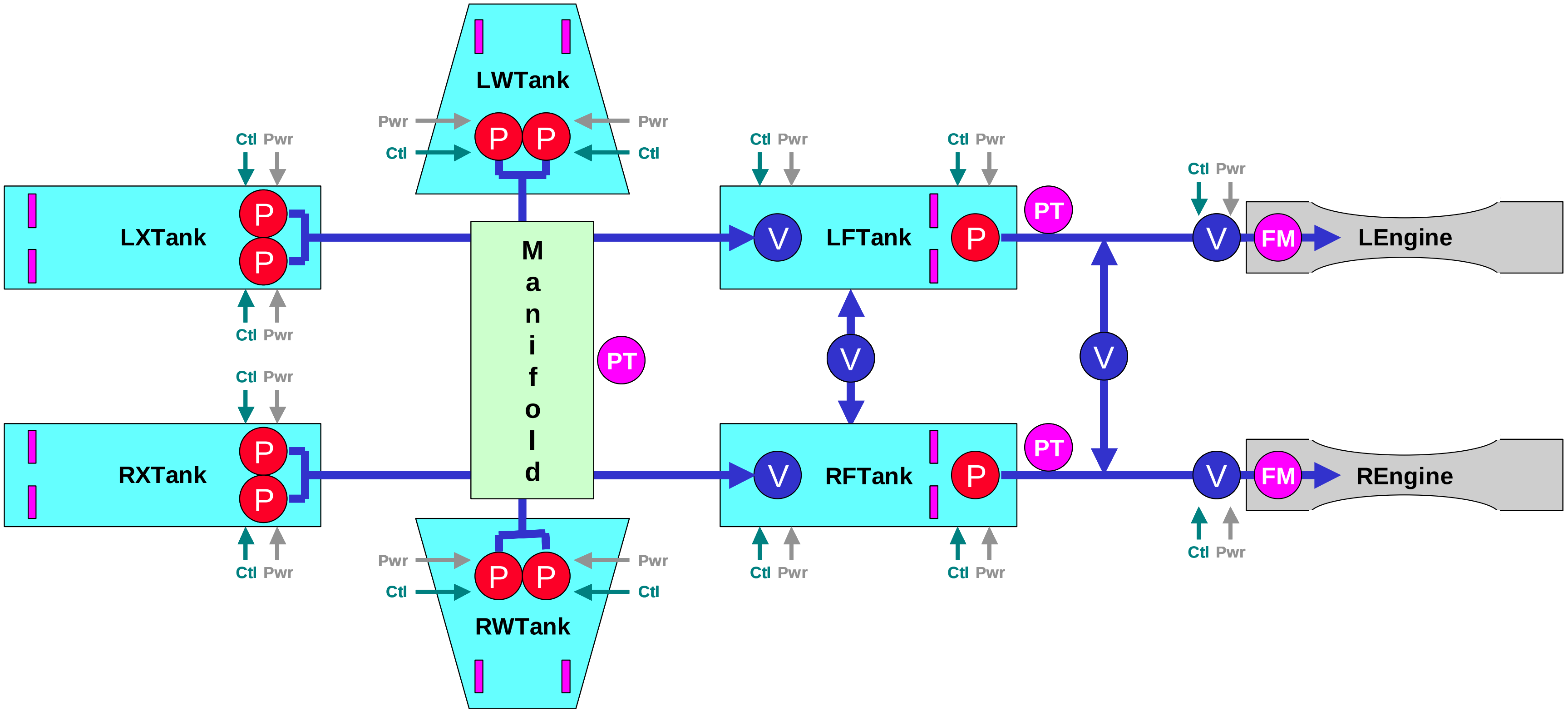
State of the art software frameworks support the integration of model-based diagnostics and prognostics into aerospace vehicles by providing a layered, “unbundled” architecture.

MBHM Reasoning Frameworks



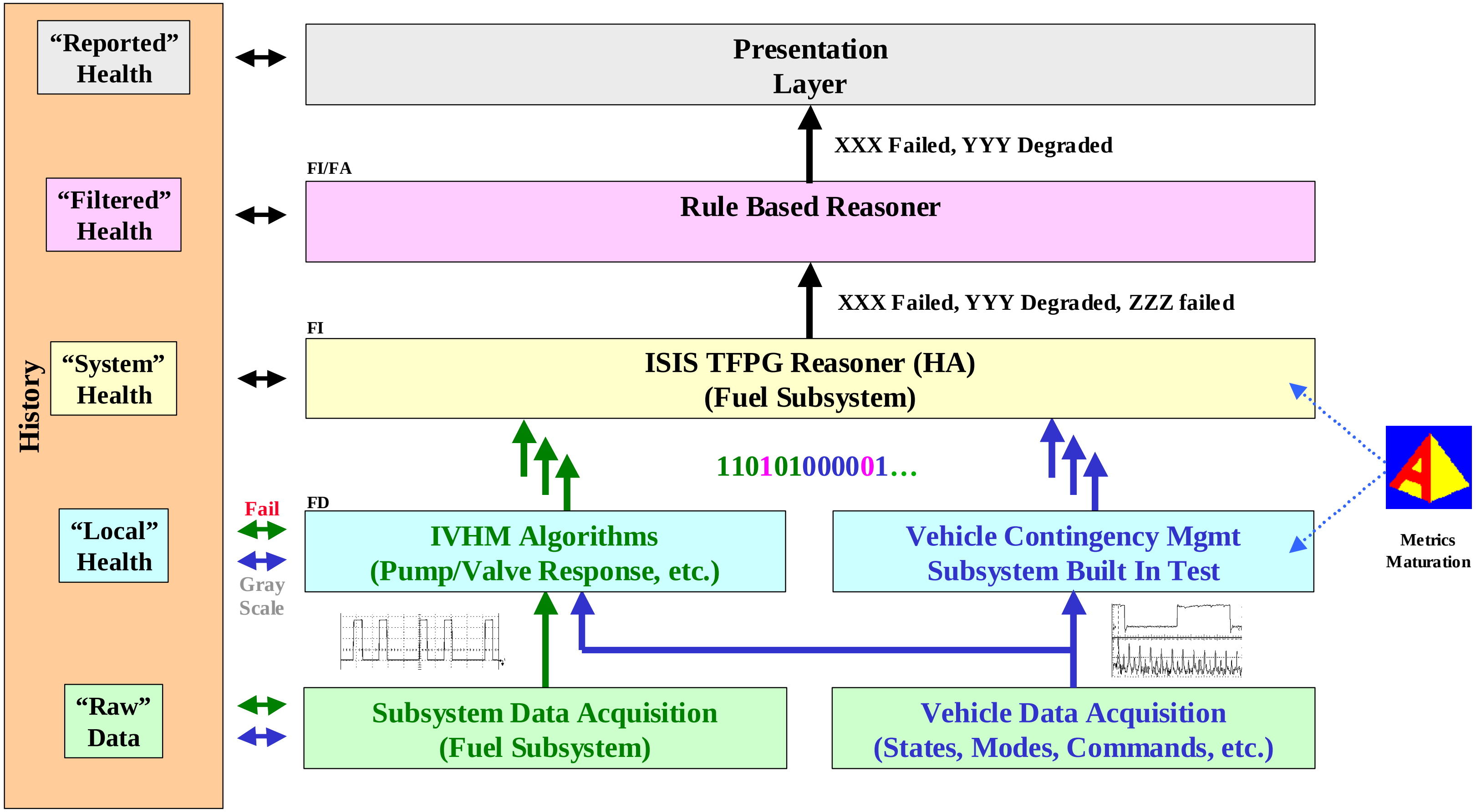
Off the shelf reasoning tools provide standardized run time engines for executing failure propagation models and/or performance models within an aerospace platform.

Case Study – Generic Fuel System



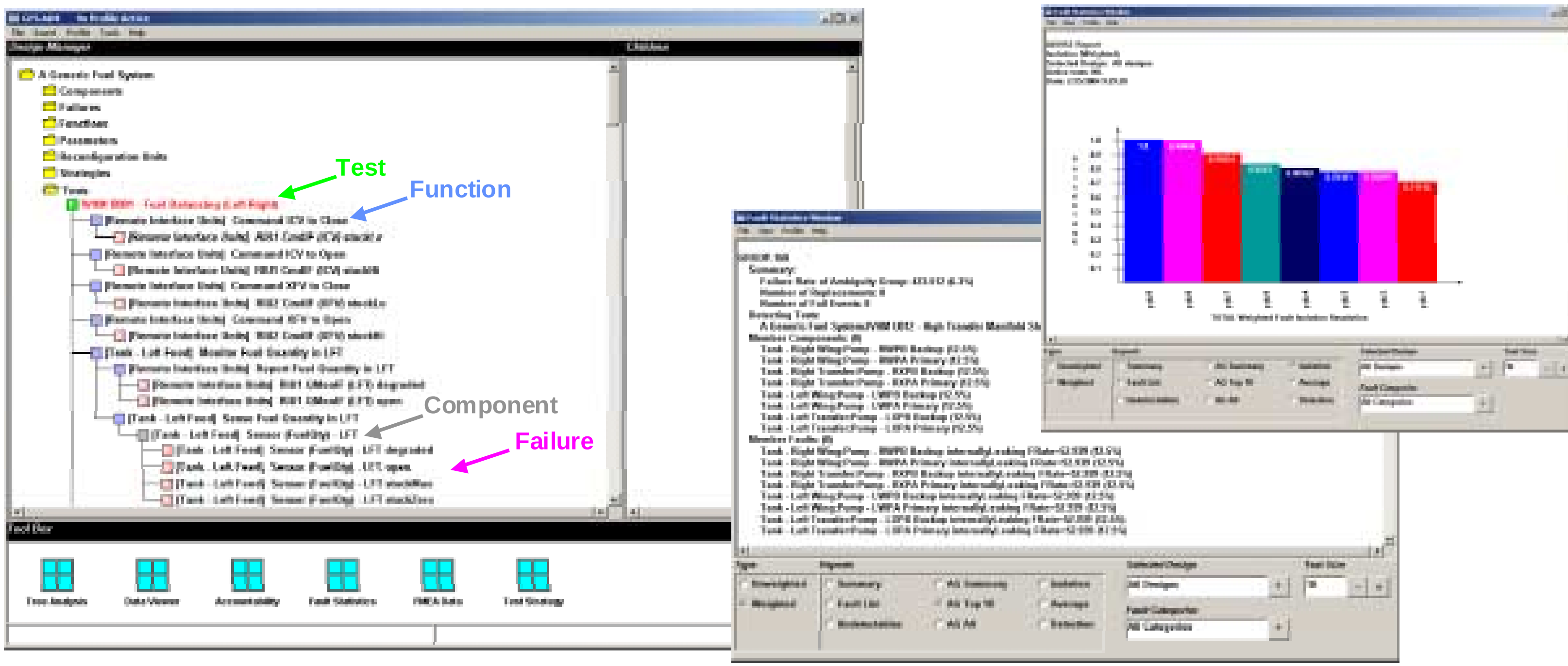
A generic fuel system (GFS) was chosen as a representative aerospace subsystem because it requires vehicle power, electronic controls, and mechanical pumps, valves, etc.

MBHM Case Study - Notional Architecture



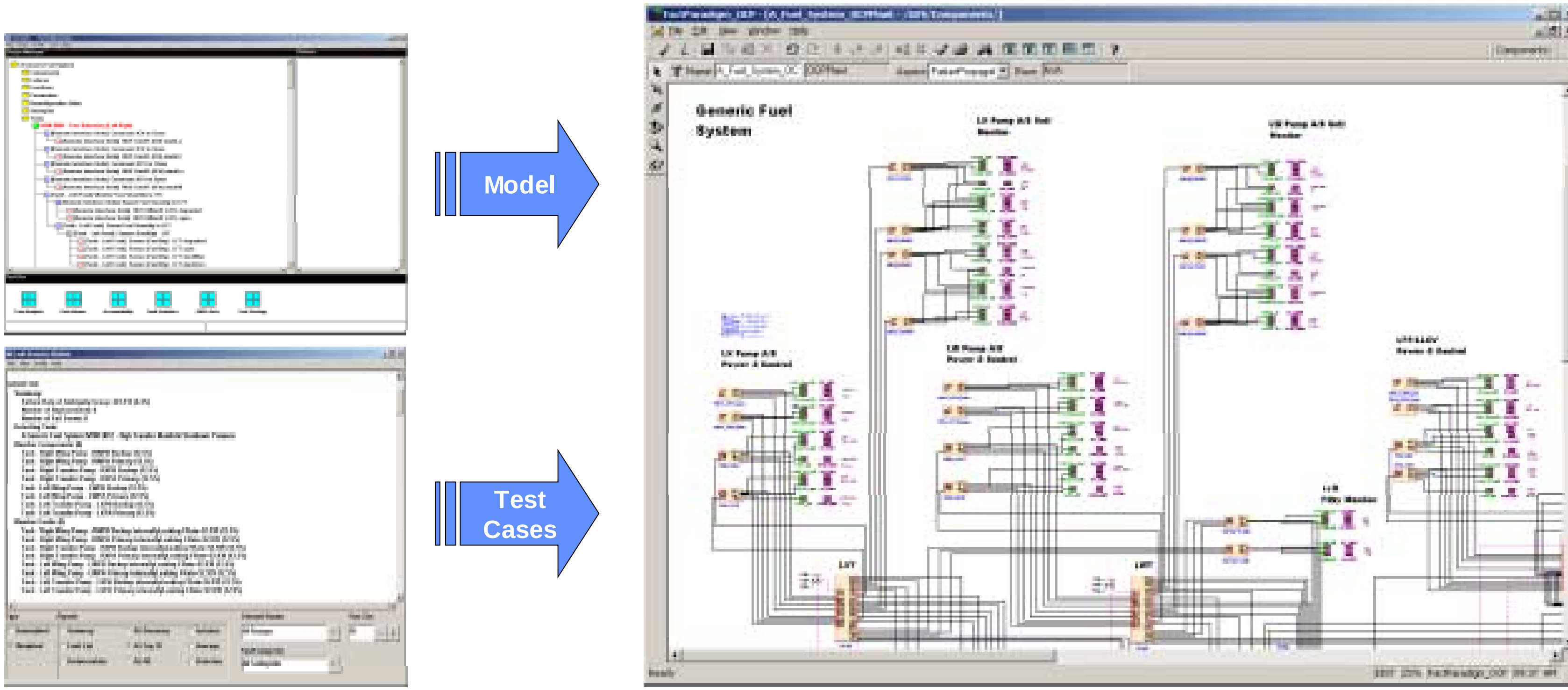
Robust GFS health assessment requires the assimilation of data from existing vehicle/subsystem monitors (e.g., BIT) as well as the outputs of dedicated IVHM algorithms.

Case Study – ADVISE Model



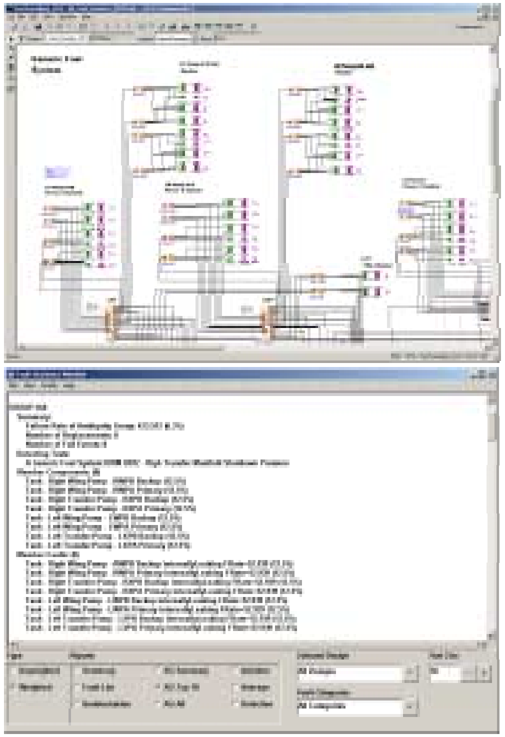
During the HW design, an ADVISE model is built to identify the sensors/tests/monitors and fault reporting logic necessary to provide the required levels of fault detection and isolation.

Case Study – TFPG Development Model



During the SW design, the ADVISE model is translated into a TFPG model using ISIS GME/FACT tools and ADVISE outputs are used for engineering desktop validation of proper diagnosis.

Case Study – TFPG Run Time Model



Model →

Test Cases →

TFPG Domain Model (C++ Code)	Fixed TFPG Engine (C++ Code)

During the SW design, the OSA-CBM compliant TFPG run time code is automatically generated and the test cases are reused for SW desktop validation of proper run time diagnosis.

Practical Experiences & Issues

Case Study Statistics

- **244 unique ambiguity groups identified by ADVISE**
  - Static diagnosis using all defined tests, single fault assumption.
- **320 test cases used to verify run time diagnosis**
  - Dynamic diagnosis using currently reported failures.
    (e.g., some tests can only be run in certain modes or at certain rates)
  - Account for failure mode dependencies.
    (e.g., a valve can't be stuck open and stuck closed at the same time)
  - Account for multiple failure scenarios.
- **ADVISE to TFPG Translation**
  - Manual TFPG model required several weeks of labor and was 82% "accurate" on first try.
  - Translated model will require a few hours of labor and should be 100% accurate on first try.
  - Translated model was slightly smaller and faster.
  - Batch scripts automatically generate the necessary data sets for TFPG model/code testing from the ADVISE ambiguity group report
- **Run Time Performance (target PPC processor / VxWorks / C++)**
  - Real time diagnoses will be run in an event driven manner
    - Event = mode change or monitor status change
  - Test cases averaged < 0.5 seconds of CPU time per event (max 1Hz rate anticipated)
  - Four large models run simultaneously with nearly linear memory & throughput demands

Summary

- **IVHM requires rigorous systems engineering to manage complexity and assure integrity.**

- **A model-based approach provides a disciplined methodology for supporting the SE process:**
  - **Successive refinement of diagnostic concepts and implementation.**
  - **Incremental transition from conceptual design to detailed design to validation.**
  - **Reuse of engineering data/models across design cycles.**

- **The Boeing Company is currently implementing a process-based, model-driven approach by employing tools from Boeing and ISIS, while evaluating other reasoners.**

- **The GFS case study is being used to document and benchmark the basic steps in the modeling process.**

- **Integration of the run time reasoners and models into Boeing’s desktop software development environment is on-going.**