Jet Propulsion Laboratory
California Institute of Technology

Top Recent Advances in ISHM

for Robotic Spacecraft

- ISHM contributions to making spacecraft more autonomous
- FM’s role in Model-Based Systems Engineering (MBSE)

Autonomous Spacecraft

Today

- **Heavily dependent on ground**
  - uploads "low-level" command sequences & parameters
  - controls when major events (e.g. ΔVs) occur
  - ground-based ephemeris generation
  - limited onboard reasoning
- **Fault management philosophy**
  - "Save the vehicle, we'll get data later!!"
  - detect faults; let ground isolate & recover
  - place S/C in pre-determined safe configuration

Tomorrow

- **Hands-off interaction**
  - goal-directed commanding
  - onboard, high accuracy navigation
- **Increased onboard reasoning**
  - let S/C determine when to do major events
  - let S/C manage its assets & make more decisions
- **Fault management philosophy**
  - Onboard fault isolation
  - Onboard fault recovery & resolution
  - "Fly-through the failure & continue gathering data!!"

Current FM Approaches are remarkably similar

Recognized at NASA Fault Management (FM) Workshops

- **Hardware Checks**
  - **Watchdog timers, heartbeat checks**
  - **H/W overspeed detectors, undervoltage trips**
- **Simple Rules**
  - **If A > threshold -> set flag = true**
  - **Emphasis on fast, accurate, easy to categorize symptoms**
  - **Examples include pointing error, attitude rates, voltage, temp …**
- **"Processing" Rules**
  - **Perform some low-level processing of data to assess situation**
  - **Example (1) If gyro reading = constant for too long -> set flag = true**
  - **Example (2) Process earth sensor data to determine loss of nadir**
- **Single "Model-Based" Rules**
  - **If f(x) > threshold -> set flag = true**
  - **Use system knowledge to calculate some expected behavior**
  - **Examples include total system momentum, reaction wheel rates**

These methods all lack Health State Information

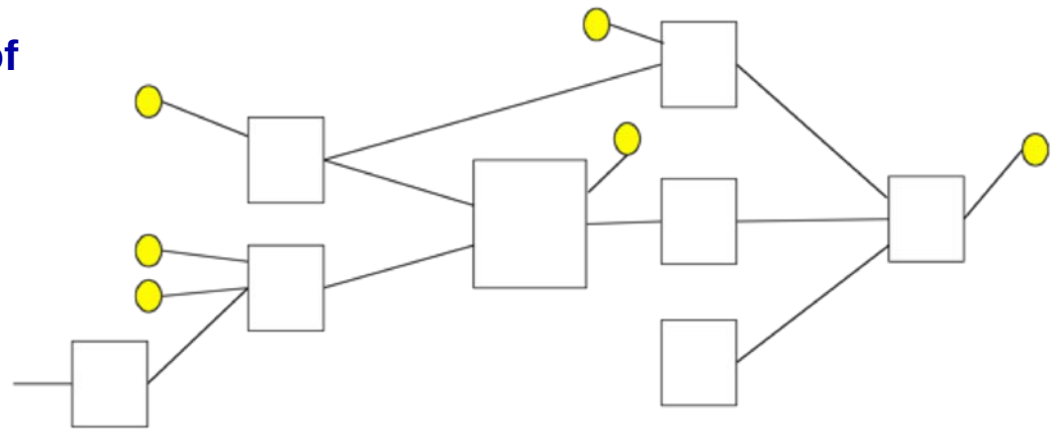
On-Board Diagnosis

- **System-level diagnosis is difficult**
  - **Many failure modes, interactions, probabilities**
- **Ad hoc symptom-to-suspect associations likely to have errors of omission and ranking**
  - **Detection oriented instead of isolation oriented**
  - **Focus limits the ability to deal with “complex” anomalies**
  - **Limits overall level of onboard autonomy**
  - **Forces humans to be in the loop**
- **A sounder approach: System-wide Model-based Reasoning**
  - **Code how each device behaves nominally**
  - **Connect them together**
  - **Diagnose from first principles**

System-wide Model-Based Reasoning

Compares values from multiple sensors

- **Use detailed knowledge of system to detect faults**
- **View system as a collection of components with inputs, outputs, & sensors (●)**
- **From engineering & experience, know fundamental behavior of each component**
- **Behaviors are called constraints**



Generic Network Model

Currently, Okean Solutions is developing MONSID model-based approach through a NASA SBIR Phase II effort

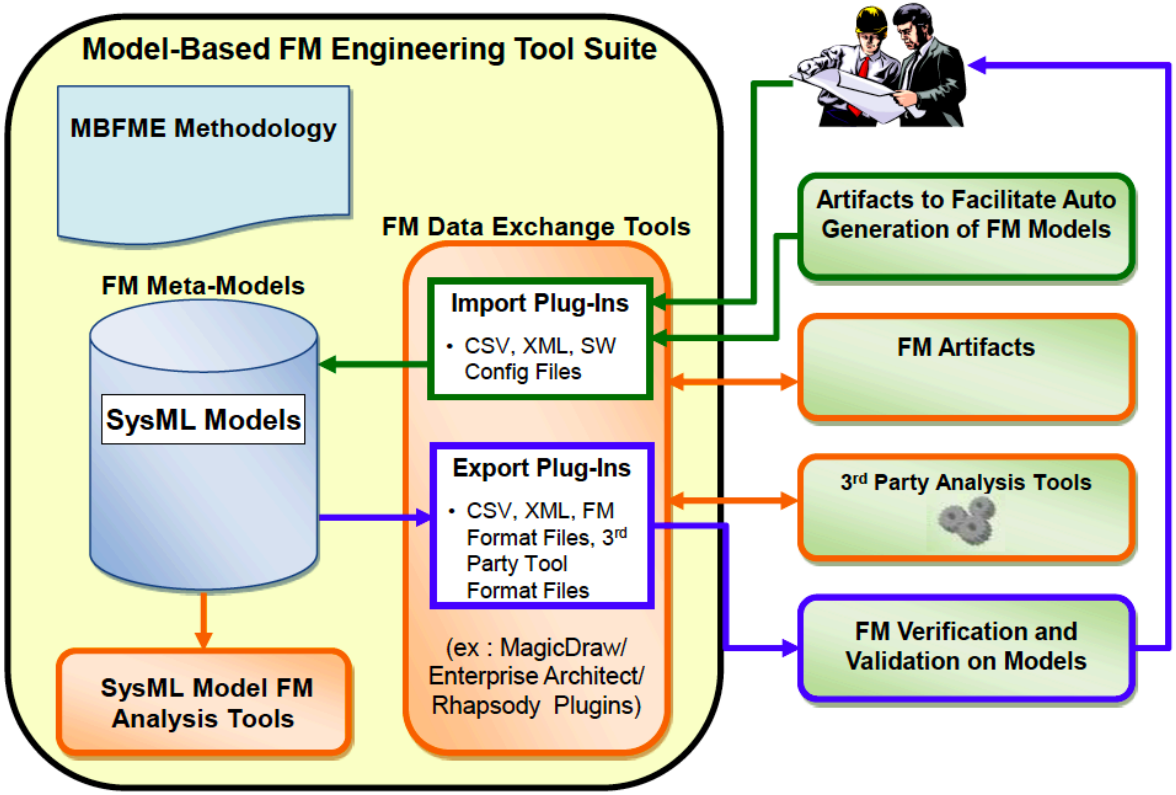
Summary and next steps

- **System-wide model-based ISHM approaches to provide health state information needed for autonomy**
  - **Diagnosis based on a few principles of causality**
  - **Algorithm handles complexity, not programmer**
  - **Model-Based approach encourages methodical device coverage**
  - **Device models easy to write and inspect**
  - **Result: System-level diagnosis more complete and correct than with symptom-to-suspect rules**
- **Next Steps**
  - **V&V**

FM's role in MBSE

Model-Based Fault Management Engineering (MBFME) Tool Suite

Tietronix Software currently is developing the MBFME Tool Suite under NASA SBIR Phase II contract



MBFME Tool Suite

Current efforts

- FM Meta-Model for FMECA modeling method - FM elements and relationships
- FMECA MagicDraw plug-in
  - extracts details about failed states
  - Traverses behavior diagrams to determine potential end effects for analysis
- FM Meta-Model for Fault Tree modeling method
- Fault Tree generation plug-in
  - Extracted FTA expected output from the models
  - Generates a graphical display of the fault tree
- Library of Reusable SysML FM Elements

Jet Propulsion Laboratory
California Institute of Technology