

# NIST Industry Forum

08 May 2018

## Crafting Intelligent Systems Management Using Requirements-Driven Design

Mark Walker D2K Technologies

[mark.walker@d2ktech.com](mailto:mark.walker@d2ktech.com)



# Agenda

- ◇ Intro
- ◇ PHM Overview
- ◇ Requirements Driven Design
  - ◇ Definitions
  - ◇ Generic Approach
- ◇ Re-usable OO Platforms
  - ◇ Overview
  - ◇ Architecture





# Who Are We?

- A **Solutions** company established in 2014, D2K utilizes:
  - reliability centered design methodologies
  - state of the art **OO AI** software development platforms  
(we love reuse!)
  - agile software engineering for on-time delivery of validated software solutions
- **Focus: to leverage system model-based reasoning for delivering “Situation Aware” software. SA software is “thinking” software that encapsulates insight and understanding regarding operation, availability, uncertainty, and adaptation.**
- ...software that can intelligently and autonomously **monitor, control, emulate, execute, or optimize** actions that will successfully ensure safe, timely, and dependable results.



# Prognostics and Health Management (PHM)

## PHM Systems are evolving to meet higher expectations

- **What should PHM Systems do?**
  - Determination of Health and its impact on system functions
  - Monitor early warning of incipient failures
  - Predictions of Remaining Useful Life
  - Leveraging of advanced “reasoners”
    - Signal processing for event detection
    - Algorithms for event correlation and sensor fusion
    - Expert Systems and rule-based architectures
    - Advanced neural and statistical classifiers
    - Real-time state estimators
    - Model-based Reasoning
  - Supervisory-level intelligence / logic
  - Estimation and understanding of system state within operational context
  - Decision support to assist operators in maintaining operational availability
  - Optimize scheduling of maintenance and corrective actions according to the principals of condition-based maintenance



# Prognostics and Health Management (PHM)

- **How have PHM Systems performed?**
  - Expensive
    - Takes too long to develop and deploy
  - Often ill specified
    - Limited access to existing design data
    - Incomplete (or non-existing) design data
  - Often an afterthought - considered very late in design cycle
    - Often reduced in scope
    - Or involving small incremental improvements to legacy systems
    - Or eliminated altogether
  - Excruciating test and validation cycles
    - How to qualify PHM system?
    - No false positives / no false negatives
    - Test and validation using Simulation vs. historical data vs. supervised learning
  - Questionable performance
    - Is system availability increased (downtime minimized)?
    - Is MTRR decreased?
    - Are operators better equipped and informed?
    - Are overall lifecycle costs reduced?



# System Management Design Considerations

- **Early as possible derivation of requirements**
- **Design based on functional requirements and the mitigation of failures (Behavior Driven Design)**
- **Need to link failures to detectable events across subsystems, and diagnosis to maintenance and corrective actions**
- **Design should identify necessary instrumentation (and consequences of inadequate instrumentation)**
- **Design should consider reasoning over systems, subsystems, predictive models, usage, operational regimes, real-time and historical data – within operational context**
- **Design should offer immediate advantages for life-cycle management**



# Output of Design Methodology

- **Crisp set of System Management requirements according to operational context, functional requirements, and mission objectives**
- **Preliminary definition of critical failure modes, associated instrumentation and algorithms required to detect them, and downstream consequences (as well as the intra-subsystem event propagations that drive them)**
- **Baseline system object model required for reasoning**
- **Baseline fault models for diagnosis and prognostics**
- **Simulation and initial validation of diagnostic approaches and understanding of underlying event propagation**



# Quest for Software Quality

## ◇ **Test Driven Design (TDD)**

- ◇ Write a test that fails
- ◇ Code until it passes
- ◇ Refactor (re-coding if it breaks)

## ◇ **Behavior Driven Design (BDD)**

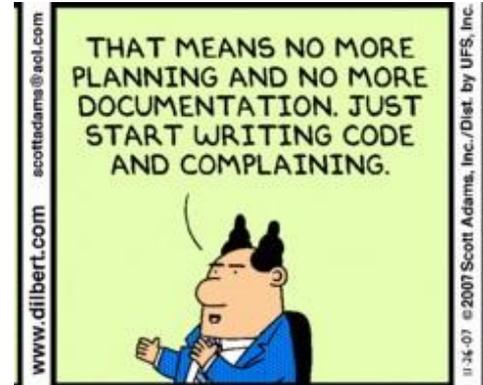
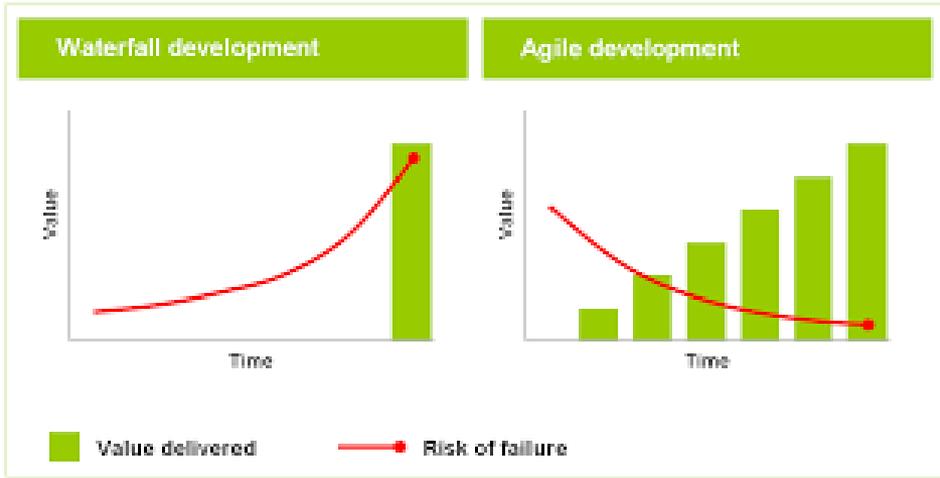
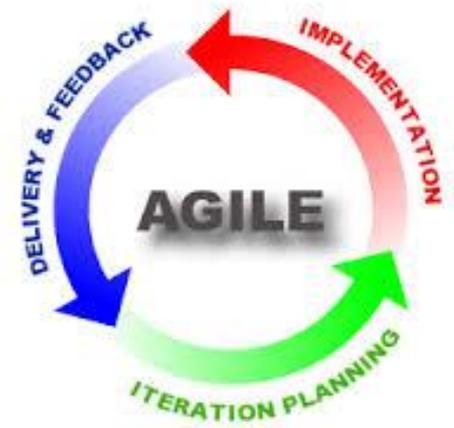
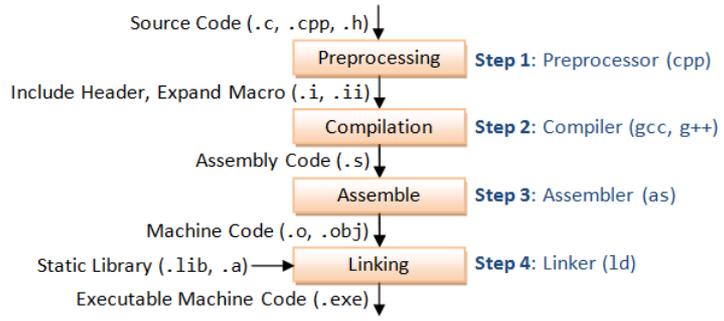
- ◇ “BDD is about implementing an application by describing its behavior from the perspective of its stakeholders”
- ◇ Requirements as User Stories
- ◇ Pull vs. Push based

## ◇ **Automated Testing using philosophy of JUnit, TestNG (example tools)**

- ◇ Automated Report Generation
- ◇ Tests follow system through life-cycle



# Agile Development Process

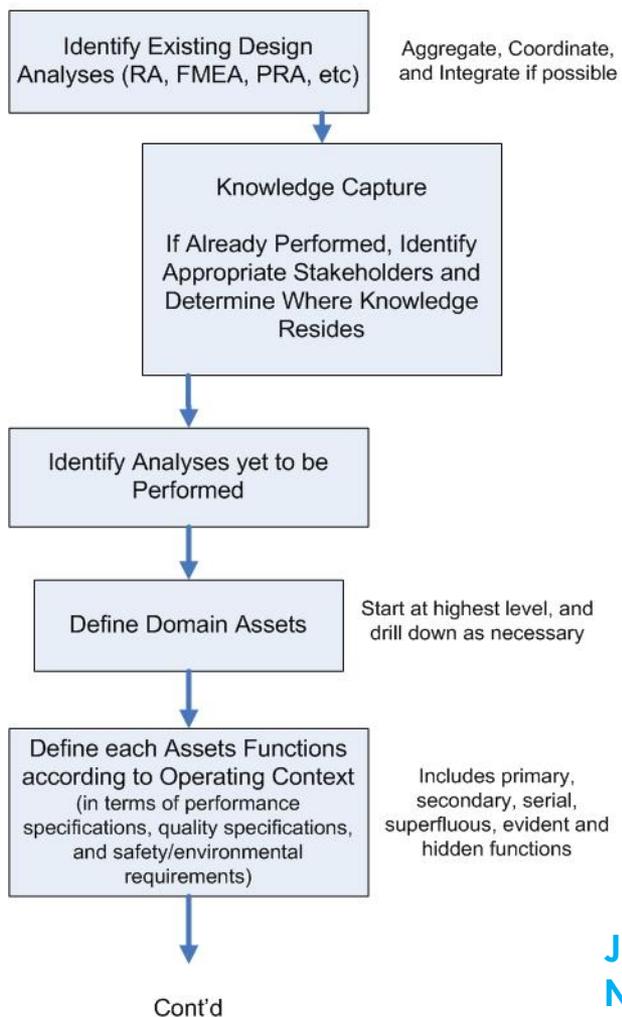




# Reliability Centered Maintenance Design

## PHM Design Methodology – Part 1

Design Analysis and Asset Definition



- **Reliability Analysis, FMEA, PRA**
- **Review content and determine if appropriate**
- **Tools and analyses should support PHM objectives.**
- **Drawings, specifications, schematics. Model to detail required by critical failure modes**

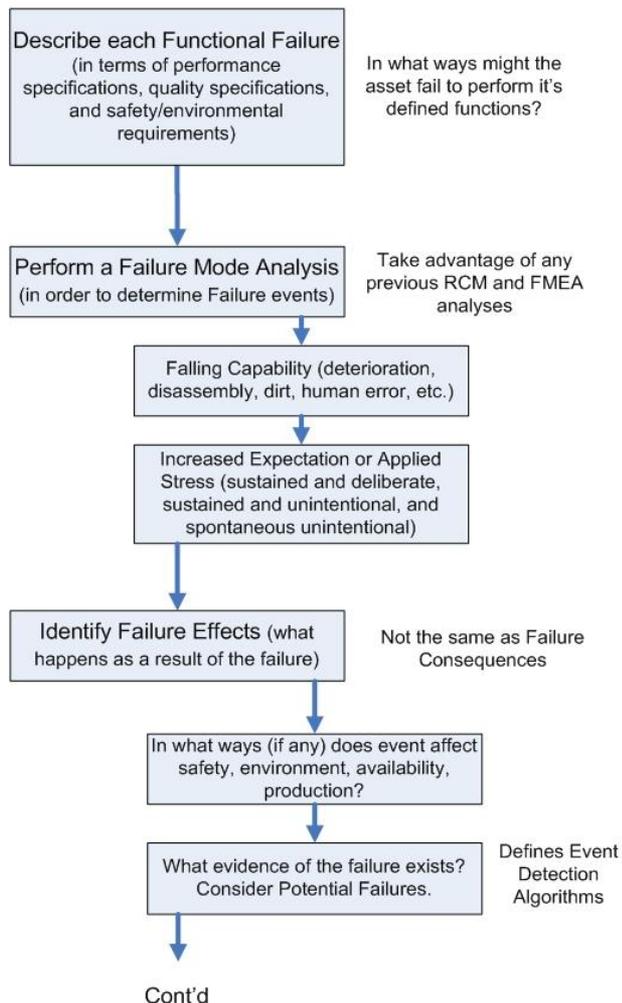
*J. Moubray. Reliability Centered Maintenance, Second Edition. New York, NY: Industrial Press, 1997.*



# Reliability Centered Maintenance Design

## PHM Design Methodology – Part 2

Functional Failure Modes and Effects



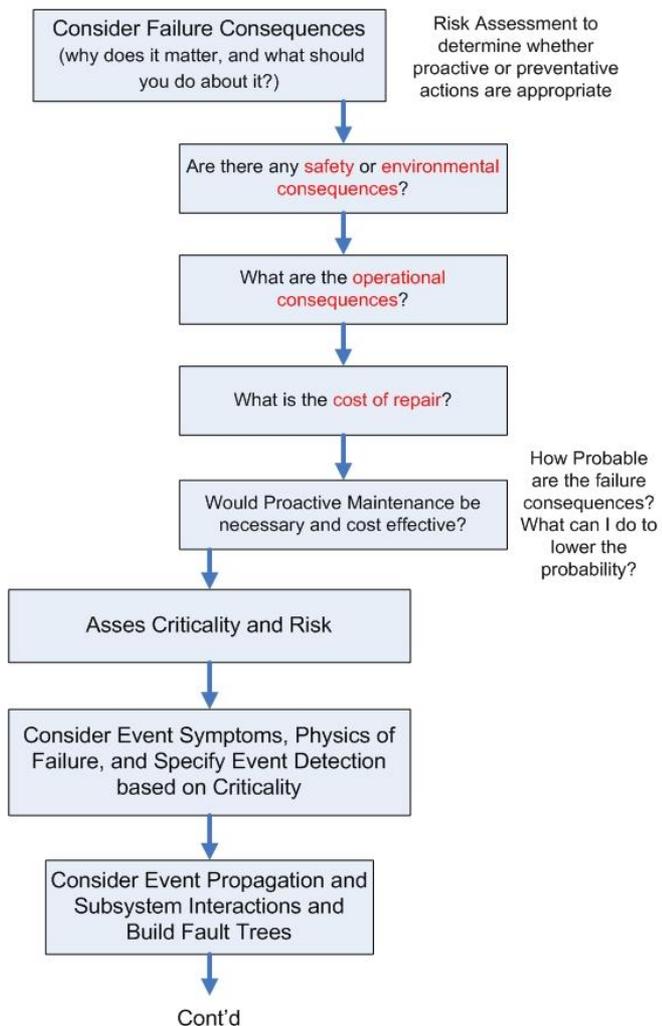
- **Functional Failure descriptions ensure that the PHM system detects what users care about**
- **Analyses may not provide insight into event propagation.**
- **Consider deterioration, increased expectation, and applied stress.**
- **What happens as a result of the failure?**
- **Take the time to consider event propagation. What evidence is available? Consider subsystem interaction**



# Reliability Centered Maintenance Design

## PHM Design Methodology – Part 3

Failure Consequences, Criticality, and Event Propagation

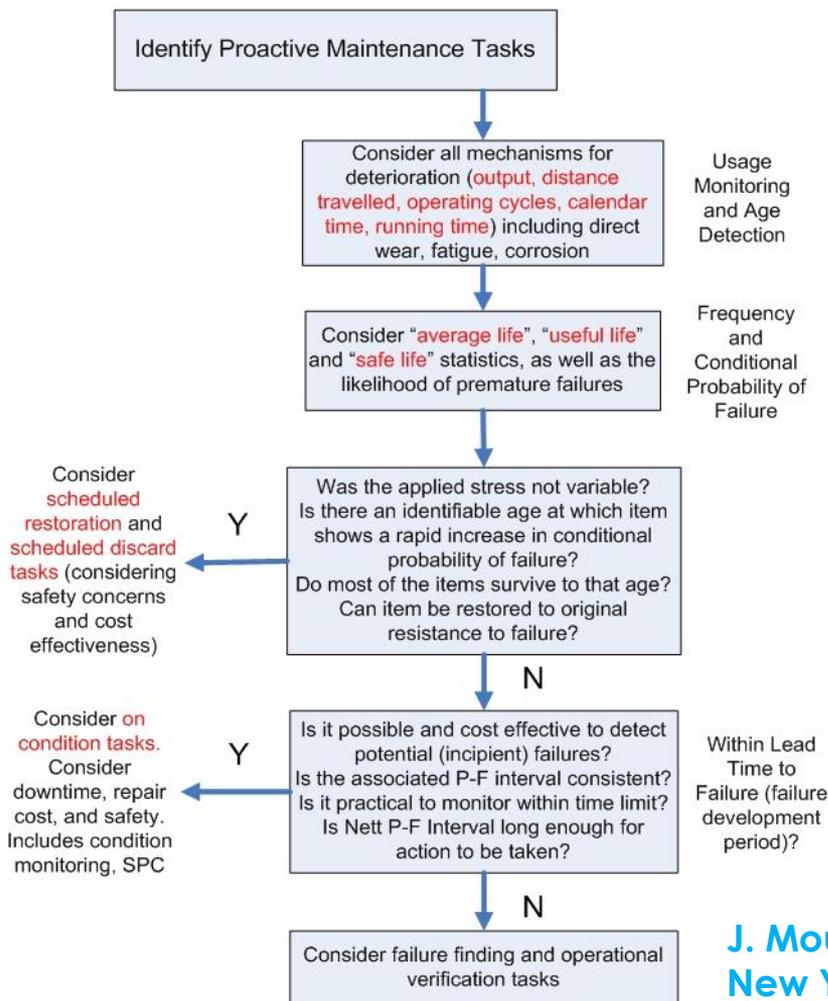


- **How serious are the effects?**
- **Did something break? Is the system down? Did something spill? Does anyone get hurt?**
- **What could be done to avoid the consequences?**
- **What insight is there for defining event detection logic?**
- **Ready to do fault modeling**



# Reliability Centered Maintenance Design

## PHM Design Methodology – Part 4 Usage Monitoring and Corrective Actions



- **Fault detection and isolation vs. Fault prediction**
- **Define the usage monitoring requirements and parameters**
- **Published, estimated, and derived statistical fault likelihoods**
- **Can failure rate be used as specified (and PM scheduled)?**
- **If possible, prognosticate**

*J. Moubray. Reliability Centered Maintenance, Second Edition. New York, NY: Industrial Press, 1997.*



# Selecting the Best Architecture

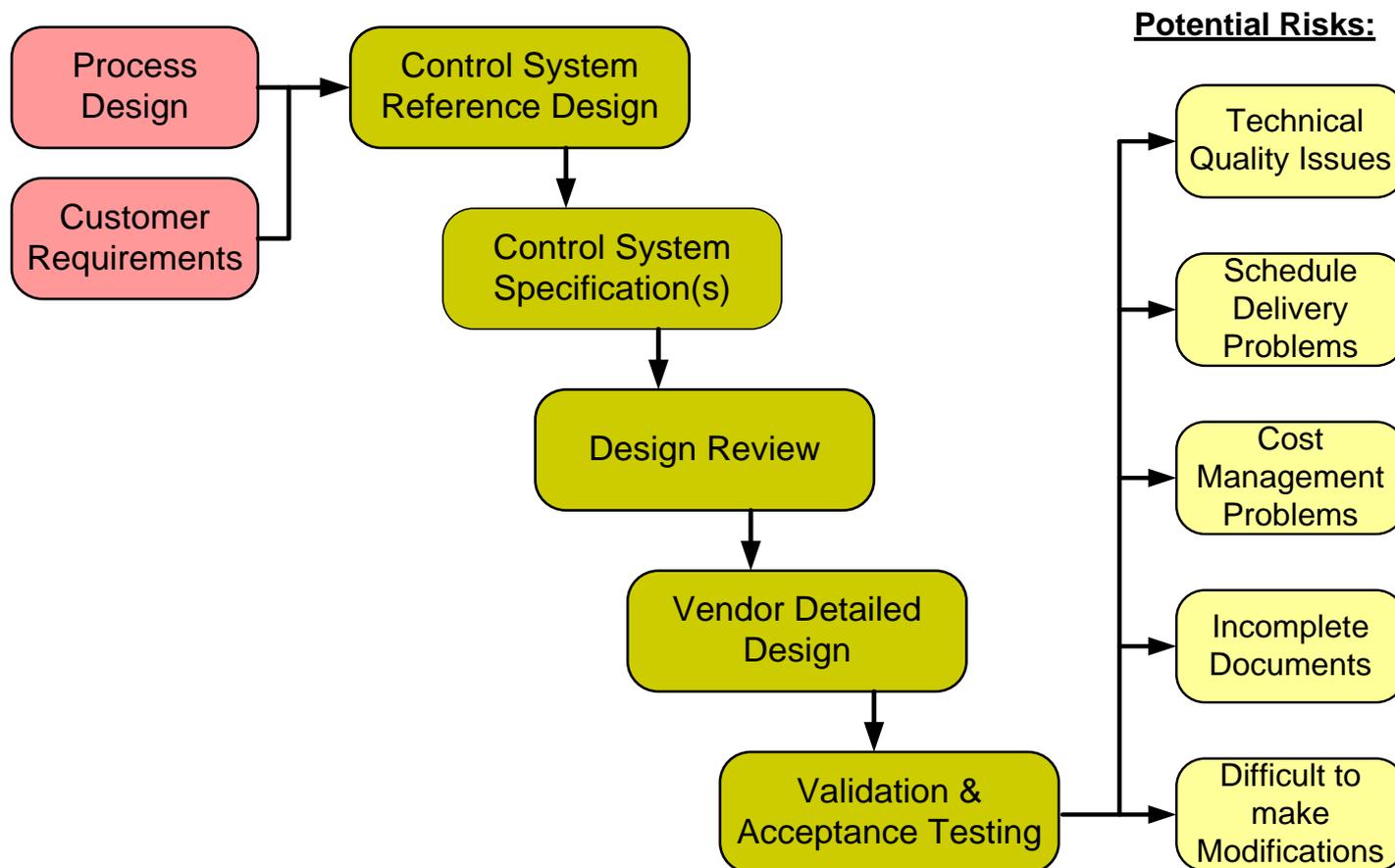
- Capabilities Abound



- How to Decide?

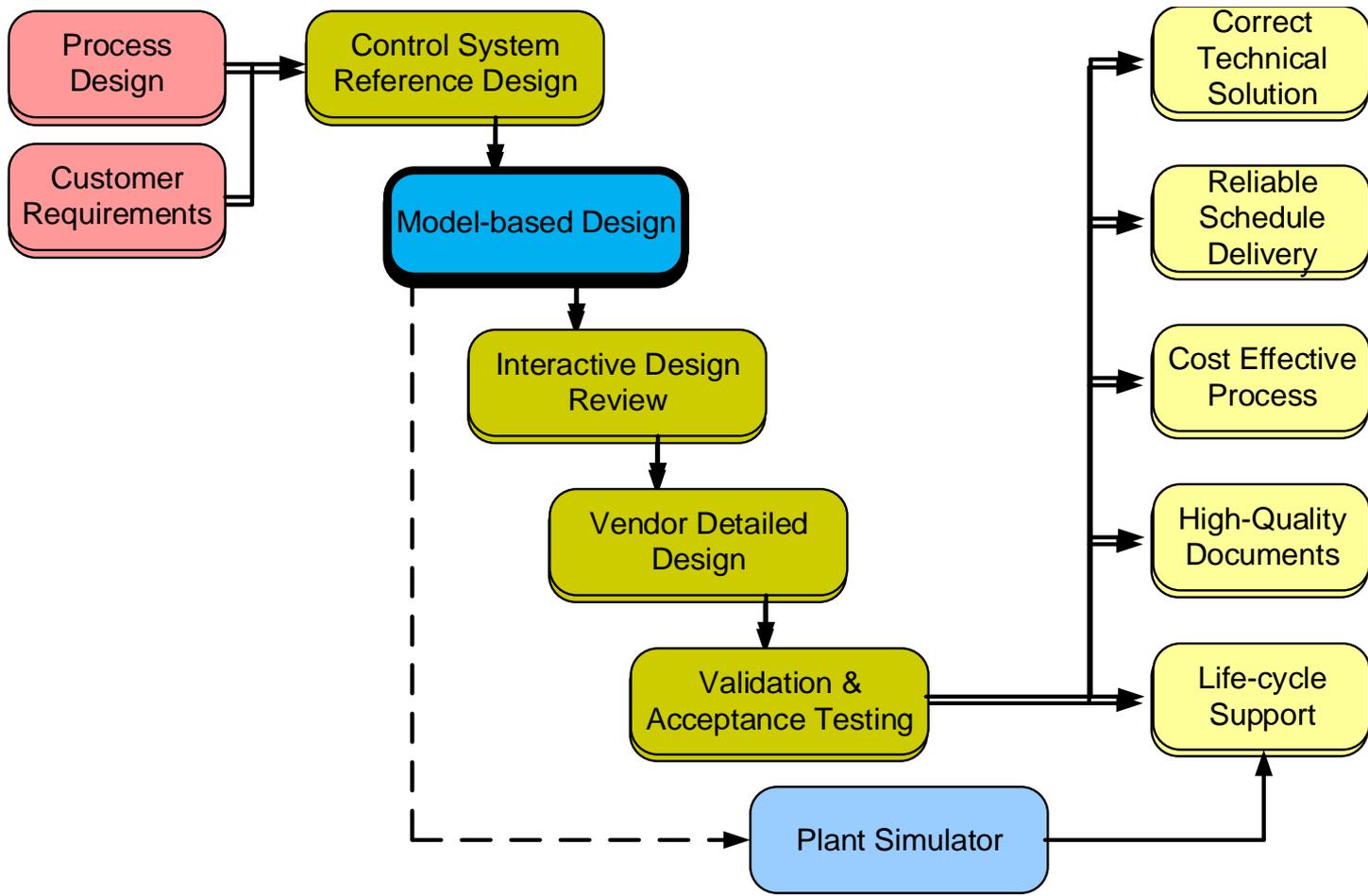


# Traditional Control System Design





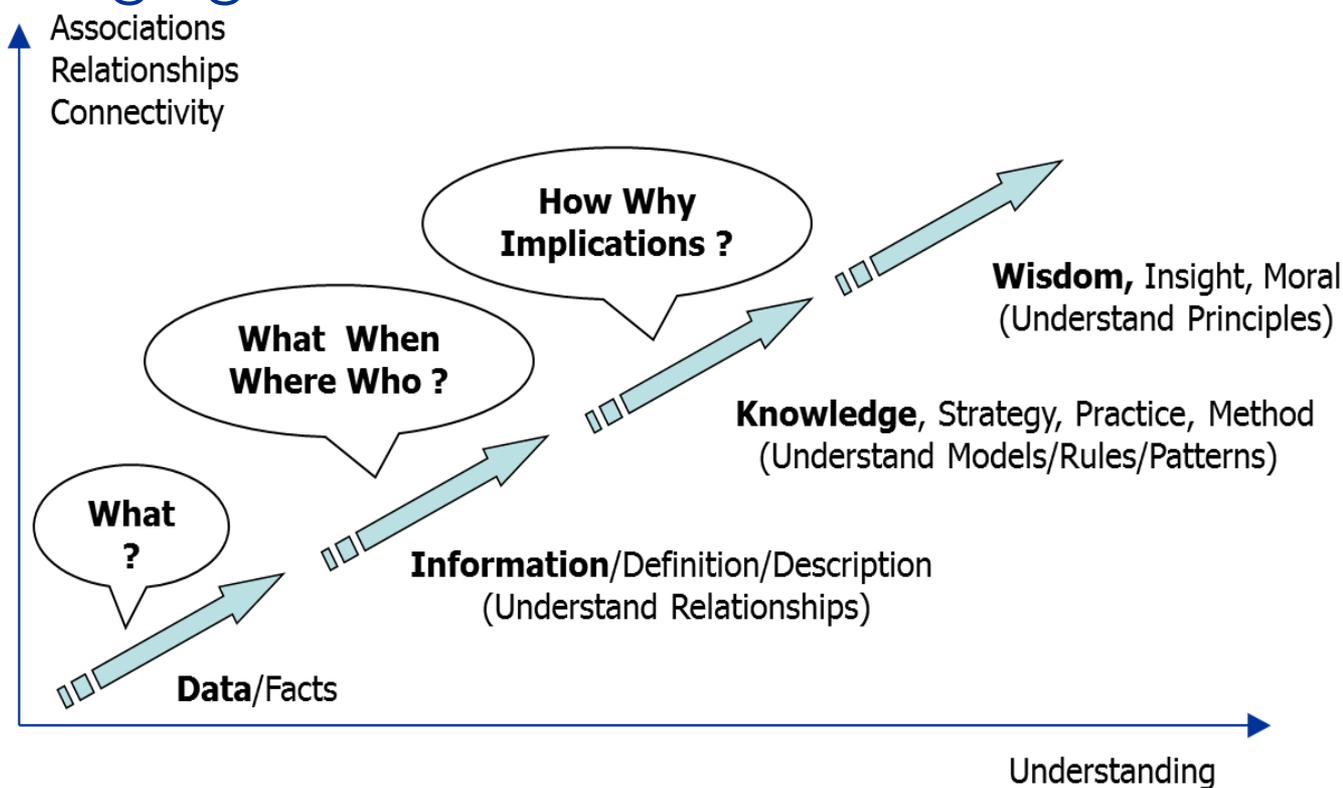
# Model Driven Design Improvements





# System Model Based Reasoning

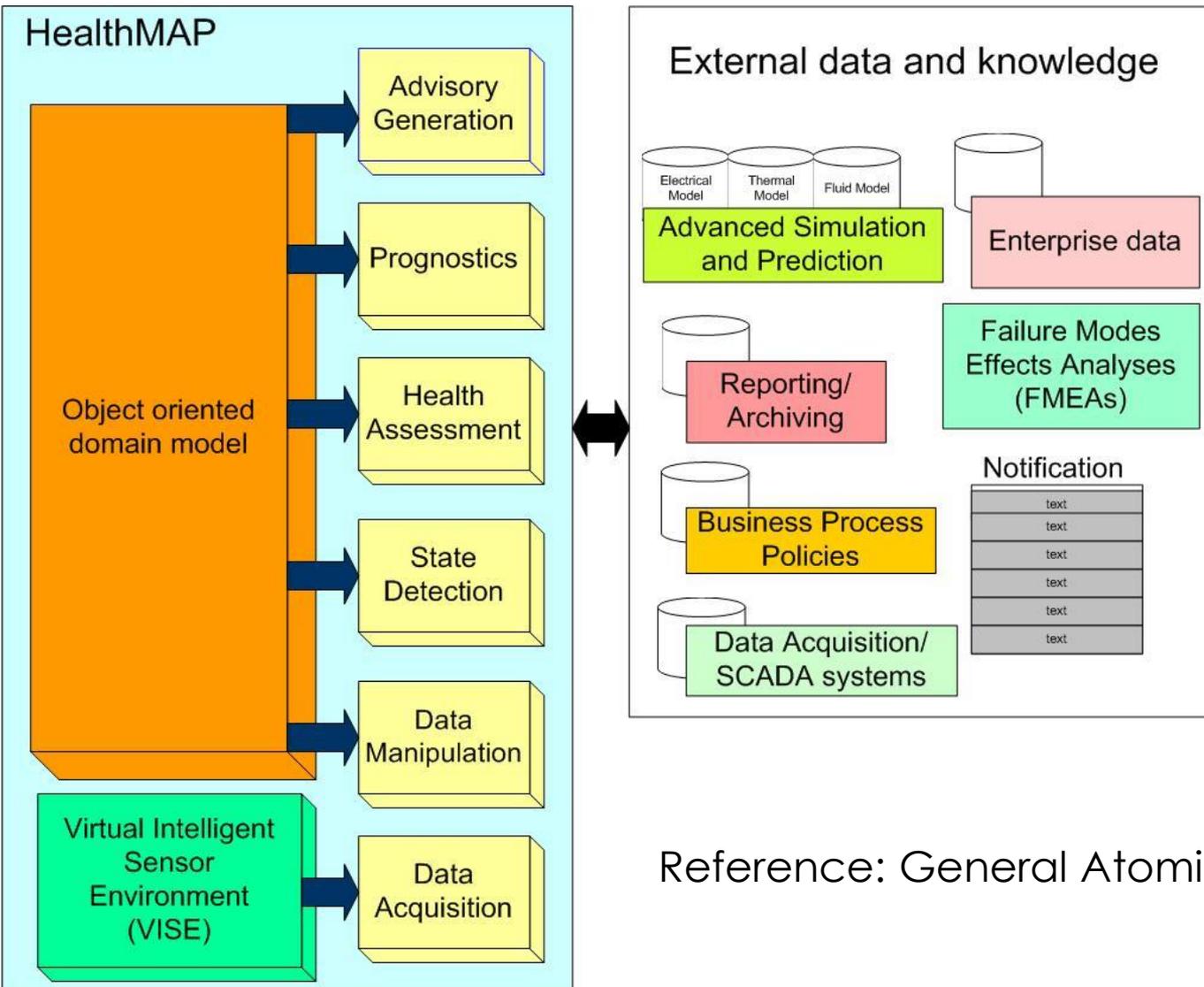
Goal: Transform data into information and knowledge based on **operational context**, leveraging all available wisdom



17

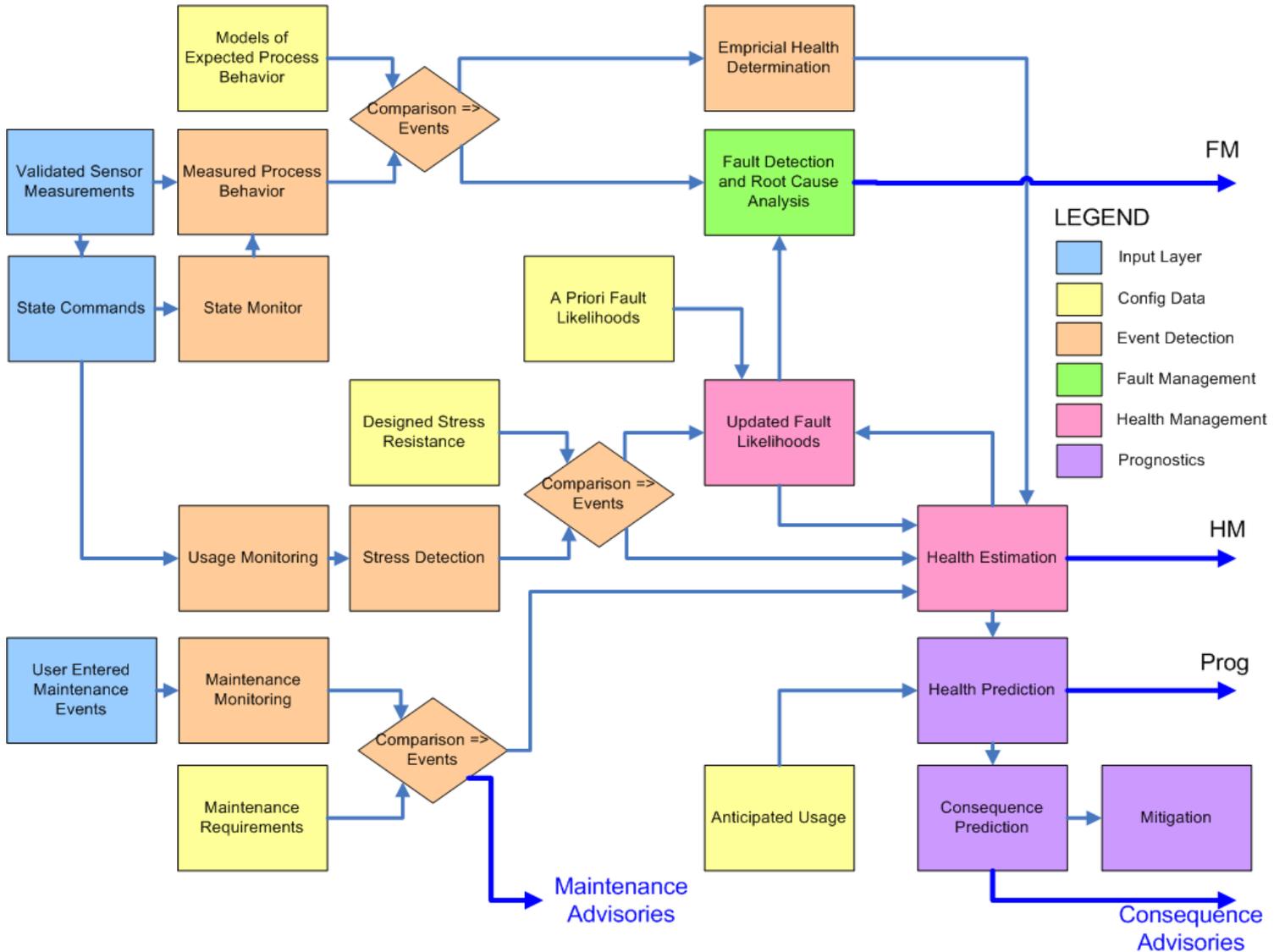


# Object Oriented Development Platform



Reference: General Atomics

# Standards-based Layered Architecture



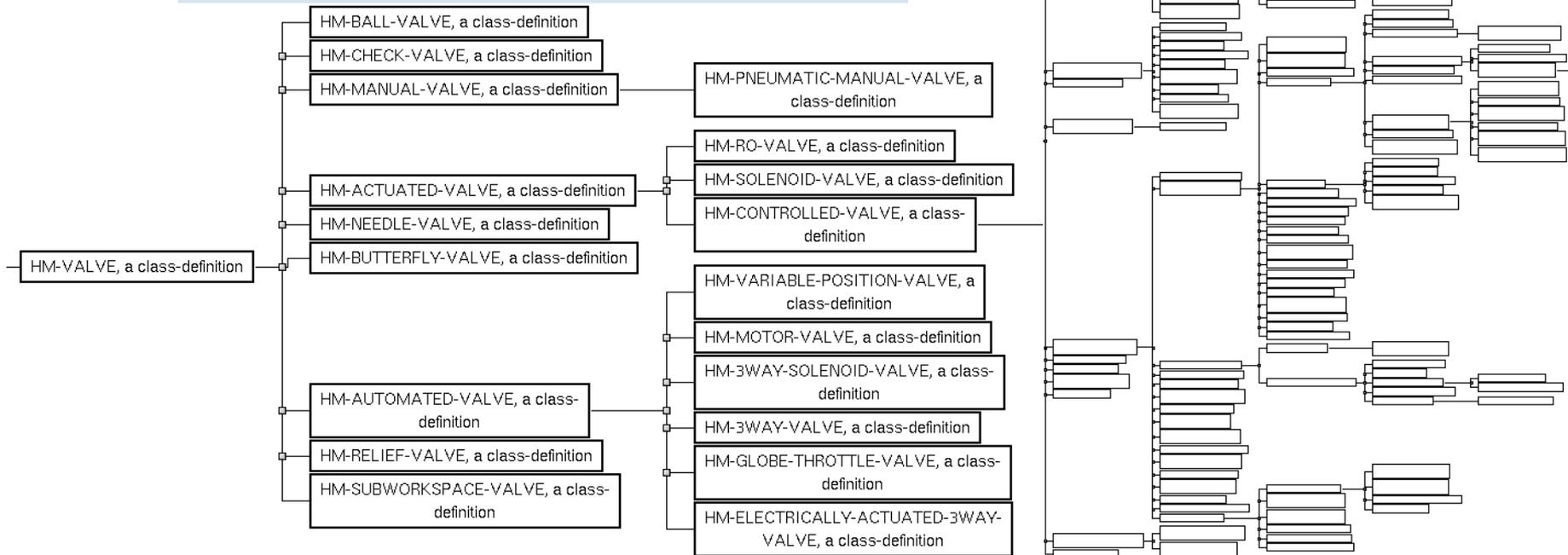
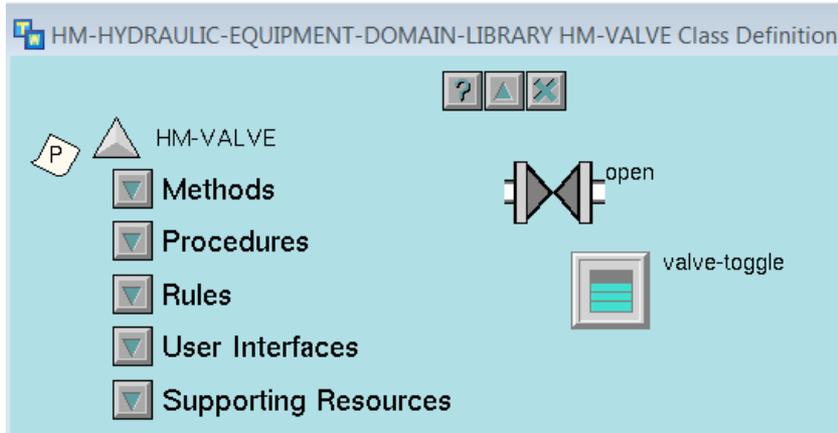


# Preferred Platform Characteristics

- **Reasoning Execution Engine**
  - Scheduling, simulation, inferencing, trending, state estimation, situational awareness, model-based reasoning, and multi-threaded processing
- **Integrated graphical modeling tools**
  - Domain representation, state transition, fault modeling, neural networks, workflow models, bow-tie diagrams
- **Methodology guided implementation using re-usable libraries**
- **OSA application supporting standards-based interfacing**
  - Transducers, DACs, PLCs, DCSs, SCADA, data aggregation platforms, 3<sup>rd</sup> party management tools, dynamic modeling and simulation platforms, enterprise data, Plant Historian, end user notification



# Complex Generic Objects with Supporting Methods





# Extensible Model Libraries w/ Palettes

HealthMAP

File Messages Console Application Domain Library Fault Models

Menu User Mode Developer Simulation

Domain Tree

- ISM-FLUID-EQUIPMENT
- ISM-GENERIC-FLOW-EQUIPMENT
- ISM-FLOW-SOURCE
- ISM-POTENTIAL-SOURCE
- ISM-GENERIC-FLOW-SWITCH
- ISM-FLOW-CIRCUIT-ELEMENT
- ISM-GENERIC-GROUND
- HM-COMPUTING-EQUIPMENT
- HM-COMPUTING-HARDWARE
- HM-MECHANICAL-EQUIPMENT
  - HM-PULLEY
  - HM-MECHANICAL-CABLE
  - HM-ROTATING-SHAFT
  - HM-BEARING
  - HM-FAN
- HM-ELECTRICAL-MACHINERY
  - HM-ELECTRICAL-EQUIPMENT
  - HM-ELECTRICAL-MACHINERY**
  - HM-UPS
  - HM-ELECTRICAL-SOURCE
  - HM-CURRENT-SOURCE

HM-ELECTRICAL-MACHINERY

HM-SERVO... HM-ROTOR HM-STATOR

HealthMAP

File Messages Console Application Domain Library Fault Models

Menu User Mode Developer Simulation

Domain Tree

- Domain Objects
  - HM-SUBSYSTEM
  - HM-EQUIPMENT
    - ISHM-PHYSICAL-SENSOR
      - ISHM-PHYSICAL-ANALOG-SENSOR**
      - ISHM-ANGULAR-POSITION-SENSOR
      - ISHM-SHAFT-ENCODER-SENSOR
      - ISHM-VIBRATION-SENSOR
      - ISHM-FLOW-SENSOR
      - ISHM-VOLTAGE-SENSOR
      - ISHM-TEMPERATURE-SENSOR
      - ISHM-CURRENT-SENSOR
      - ISHM-PRESSURE-SENSOR
      - ISHM-CONDUCTIVITY-SENSOR
      - ISHM-ABSOLUTE-POSITION-SENSOR
      - ISHM-AIR-FLOW-SENSOR
      - ISHM-LEVEL-SENSOR
    - ISHM-PHYSICAL-DISCRETE-SENSOR
  - ISHM-FLUID-EQUIPMENT
  - ISHM-GENERIC-FLOW-EQUIPMENT
  - ISHM-FLOW-SOURCE

ISHM-PHYSICAL-ANALOG-SENSOR

Angle position Shaft Enc Acc Q

ISHM-ANGU... ISHM-SHAF... ISHM-VIBR... ISHM-FLO...

V T I P

ISHM-VOLT... ISHM-TEMP... ISHM-CURR... ISHM-PRES...

uMho/cm Abs position Air flow L

ISHM-CON... ISHM-ABSO... ISHM-AIR-F... ISHM-LEVE...

HEALTH MAP hm uav oct 21

File Messages Console Application Domain Library Fault Models Coding

Menu User Mode Developer Simulation A RC

Domain Tree

- HM-HYDRAULIC-EQUIPMENT
- IS2\_PROCESS-EQUIPMENT
  - REDUCER
  - IS2\_SENSOR
  - IS2\_PIPE-SEGMENT
  - REGULATOR
  - FLOW\_SOURCE
  - FLOW\_SINK
- IS2\_MECHANICAL-EQUIPMENT
  - TANK
    - CATCH-TANK
    - SEPARATOR
    - KSC-BURSTDISC
    - A1-SC
    - DOME-REGULATOR
    - DISCONNECT
  - IS2\_VALVE**
    - ORIFICE
    - TRYCOCK
    - ORIFICE-KSC

IS2\_VALVE

2W-MANIF... DELTA-P-V... A1-FLOWM... MANUAL-V...

MOTOR-VALVE RELIEF-VALVE SERVO-VALVE VPV-VALVE

PRESSURE... CHECK-VALVE PRESS-REG... DOME-LOA...

REMOTE-O... SSC-PRESS... SOLENOID-... SSC-TEMPE...



# Domain Representations

HealthMAP hed-top-level

File Edit View Layout Go Project Workspace Tools Window Help

Menu User Mode Developer Simulation A RC M L Ready

HED System Model

Interface:

- 480V 3-phase
- 120V 3-phase
- PODS
- Discrete
- Chilled Water
- Lube Oil
- Mechanical
- Water
- Lube Oil
- DAQ

VITAL POWER

SD - 25A

SD - 25G

MCS

LBE6

E-STOP

ELECTRICAL SWBD

CONVERTER

ERM

REMOTE DAQ

CLUTCH AND BRAKE

MFG

Relation tree for DIAGNOSIS-MANAGER-0001

Flow < Fault Limit ERM-COOLING-UNIT

Flow < Fault Limit NY-COOLING-UNIT

Inadequate Flow Rate ERM-COOLING-UNIT

Inadequate Flow Rate NY-COOLING-UNIT

Loss of Supply Pressure HED-COOLING-WATER-SUPPLY-MANIFOLD-1

Failure to Remove Excessive Heat NY-COOLING-UNIT

Failure to Remove Excessive Heat ERM-COOLING-UNIT

HED Converter Schematic

SmartMAP ROOT CAUSES QUEUE

Ack	S...	Prio...	Update Time	Target	Message
		1	5/28/2018 12:59:31	Hed-Cooling-Water	Loss of Supply Pressure on HED-COOLING-WATER-SUPPLY-MANIFOLD-1



# Domain Representations

HealthMAP mq-9-top-level

File Messages Console Application Domain Library Fault Models Coding

Menu User Mode Developer Simulation A RC M L Ready

### Fuel Subsystem

LEFT-OUTBOARD-WING-TANK LEFT-INBOARD-WING-TANK FUEL-PUMP-2 FUEL-PUMP-3 FORWARD-TANK TILT VALVE HEADER-TANK RIGHT-INBOARD-WING-TANK RIGHT-OUTBOARD-WING-TANK AFT-TANK REED-TEMP-SENSOR

RETURN-SOLENOID-LEFT RETURN-SOLENOID-RIGHT RETURN-SOLENOID-LEFT RETURN-SOLENOID-RIGHT RETURN-SOLENOID-FORWARD

JET-PUMP-TEMP-SENSOR JET-PUMP-SOLENOID-LEFT JET-PUMP-SOLENOID-FORWARD JET-PUMP-SOLENOID-RIGHT JET-PUMP-PRESSURE-SENSOR

MASS-FLOW-SENSOR-TO-ENGINE

### Causal model for Leak :: return-solenoid-forward

- Lower Than Expected Fuel Level right-inboard-wing-tank
- Higher Than Expected Fuel Level forward-tank
- Lower Than Expected Fuel Level left-inboard-wing-tank
- Lower Than Expected Fuel Level aft-tank

### HealthMAP ROOT CAUSES QUEUE

Ack	S...	Prio...	Update Time	Target	Message
<input type="checkbox"/>		1	2/5/2011 14:00:58	Return-Solenoid-Left	Leak on return-solenoid-left has become true (upstream inferred)
<input type="checkbox"/>		1	2/5/2011 14:00:58	Return-Solenoid-Fo...	Leak on return-solenoid-forward has become true (upstream inferred)

HealthMAP ALERT QUEUE HealthMAP ROOT CAUSES QUEUE

# Relational Modeling Support

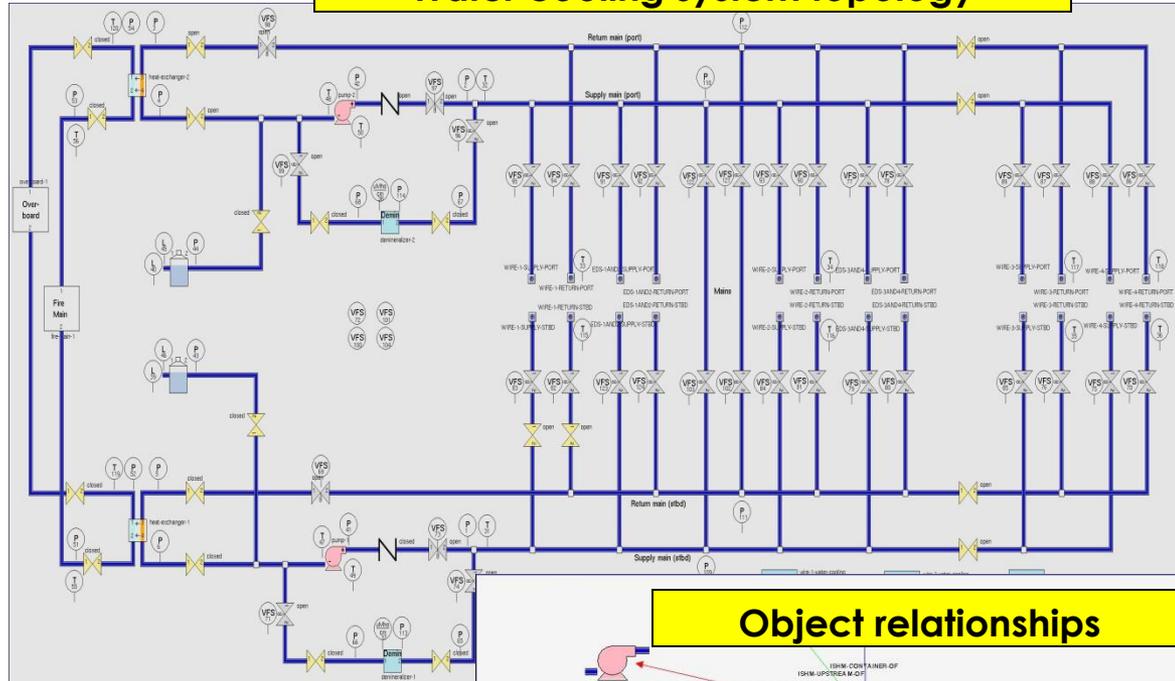
Navigator

Domain Object Definitions

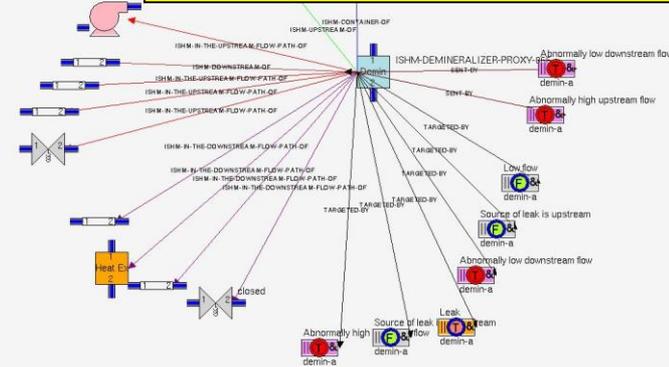
## Object Model Classes

- ISM-EQUIPMENT
  - AAG-BRAKE-HPU
  - AAG-HCU
- ISM-COMPUTING-EQUIPMENT
- ISM-ELECTRICAL-EQUIPMENT
- ISM-FLUID-EQUIPMENT
  - ISM-FLUID-GROUND
  - ISM-FLUID-PATH-ELEMENT
    - AAG-BRAKE-CARRIER
    - AAG-BRAKE-MANIFOLD-BLOCK
  - ISM-ACCUMULATOR
  - ISM-DEMINEALIZER
  - ISM-FLUID-BUS
  - ISM-FLUID-FILTER
  - ISM-FLUID-T
  - ISM-HEAT-EXCHANGER
  - ISM-MANIFOLD
  - ISM-PIPE
  - ISM-RESERVOIR
  - ISM-VALVE
- ISM-FLUID-SOURCE
- ISM-HEATER
- ISM-GENERIC-FLOW-EQUIPMENT
  - ISM-FLOW-CIRCUIT-ELEMENT
  - ISM-FLOW-SOURCE
  - ISM-GENERIC-FLOW-SWITCH
  - ISM-GENERIC-GROUND
  - ISM-POTENTIAL-SOURCE
- ISM-MECHANICAL-EQUIPMENT
  - AAG-BLANKING-PLATE
  - AAG-BRAKE
  - AAG-DRUM
  - AAG-SHOCK-ABSORBER
  - AAG-WATER-TWISTER
  - ISM-BEARING
  - ISM-ELECTRICAL-MACHINERY
  - ISM-MECHANICAL-CABLE
  - ISM-PULLEY

## Water cooling system topology

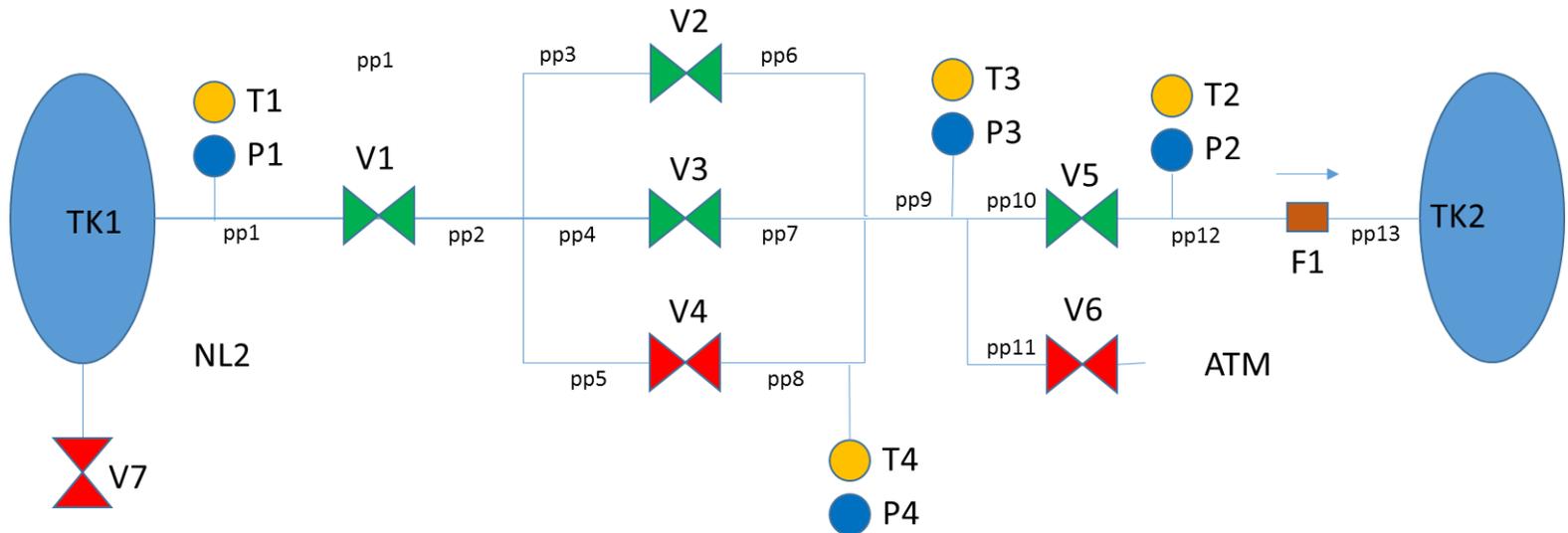


## Object relationships





# Concepts and Models



## Flow Subsystem as a Concept

Flow Subsystem 1: Members (TK1, pp1, T1, P1, pp2, pp3, V2, pp6, pp9, T3, P3, V5, T2, P2, F1, TK2), Source: TK1, Sink: TK2.

Flow Subsystem 2: Members (TK1, pp1, T1, P1, pp2, pp4, V3, pp7, pp9, T3, P3, V5, T2, P2, F1, TK2), Source: TK1, Sink: TK2.

**Note:** AO-MDS incorporates the concept of Flow Subsystem and dynamically determines Flow Subsystems for any application and its current configuration.

**In Contrast with a data/information driven approach:**

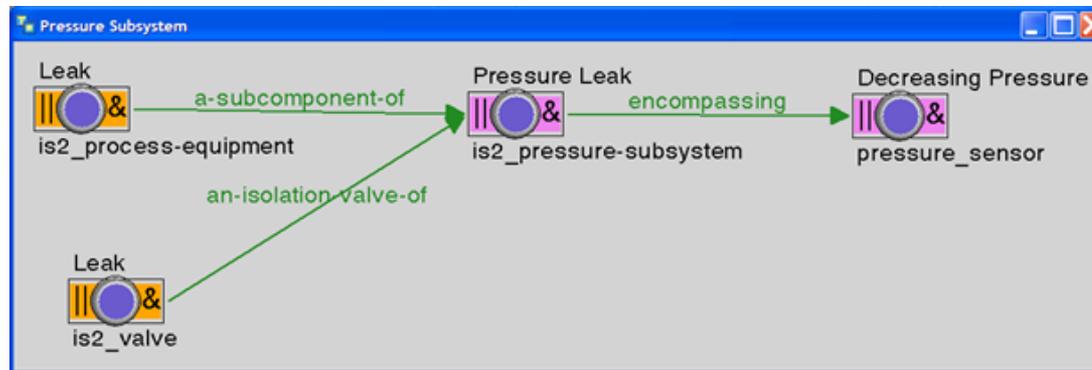
**Flow subsystem selected from a pre-defined list that considers all possible combinations of valve configurations for all schematics**

- generally hundreds or thousands of valves are involved, becoming a complex combinatorial problem.
- Any changes in the system (e.g. adding a valve) will require extensive work to update the combinatorial list.
- Any new system will require its own combinatorial list.

# Failures Modes and Effects Analysis (FMEA)

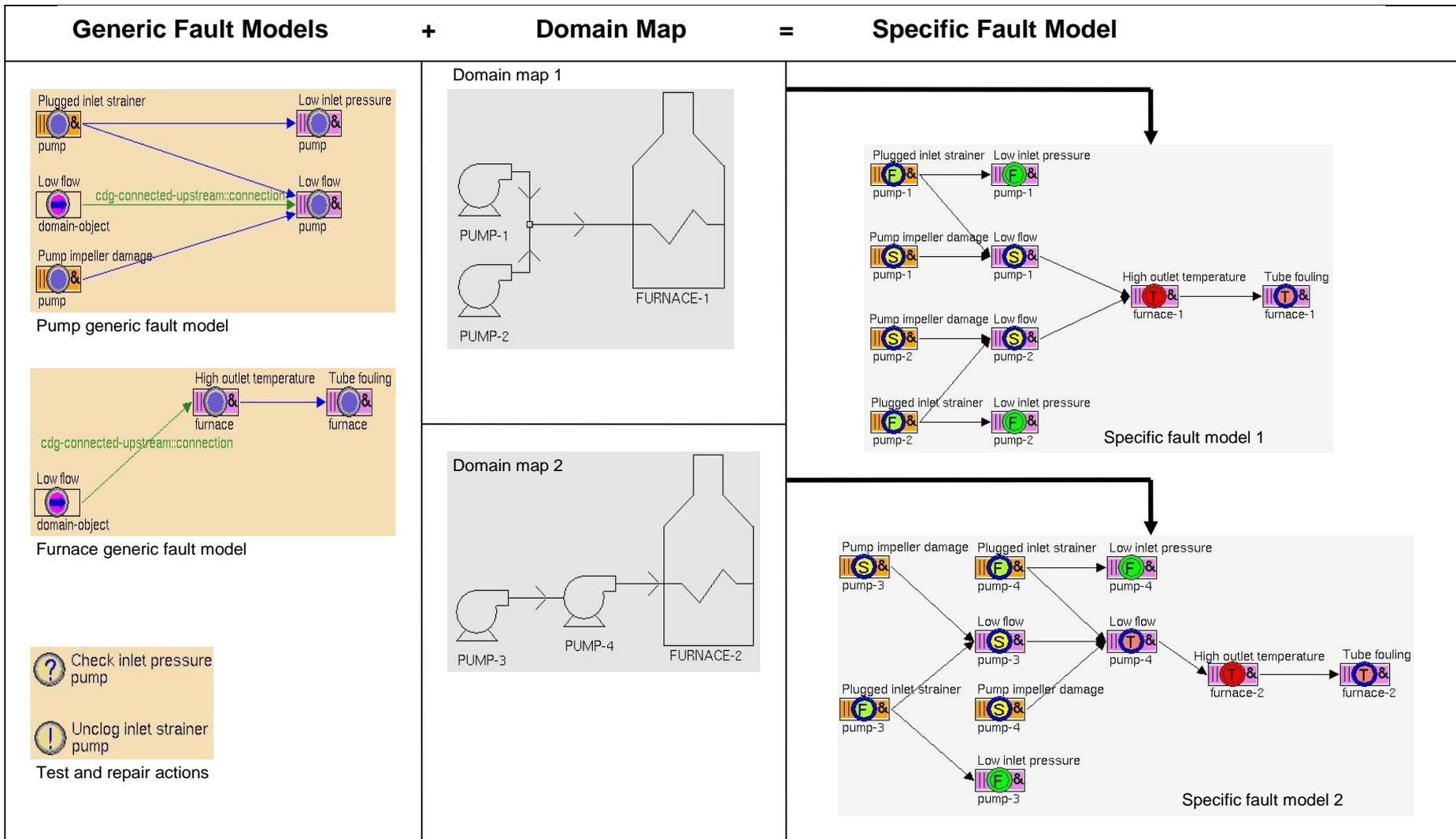
## Modeling based on MIL-STD-1629A(2)

ID #	Item-Functional Identification	Function	Failure Modes and Causes	Mission Phase-Operational Mode	Failure Effects		Failure Detection Method
					Local End Effects	Next Higher Level	
	Process Equipment	Fluid feed subsystem	Leak	Sealed subsystem maintaining pressure	Pressure leak	Decreasing pressure measurement	Identify sealed subsystem, and check pressure sensors for decreasing pressure.





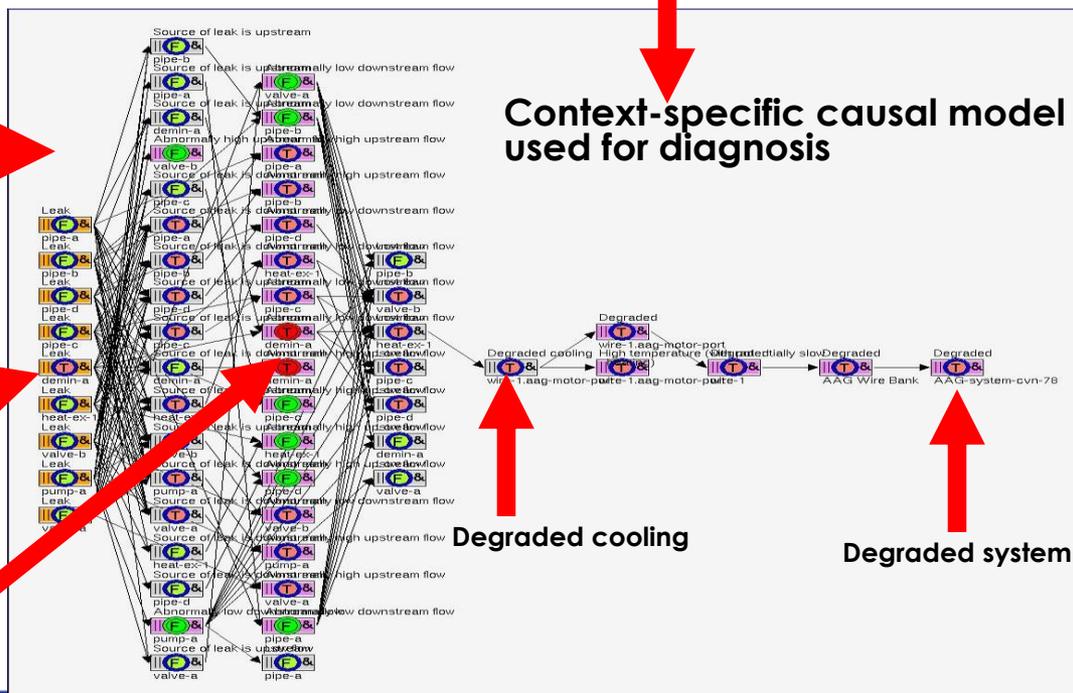
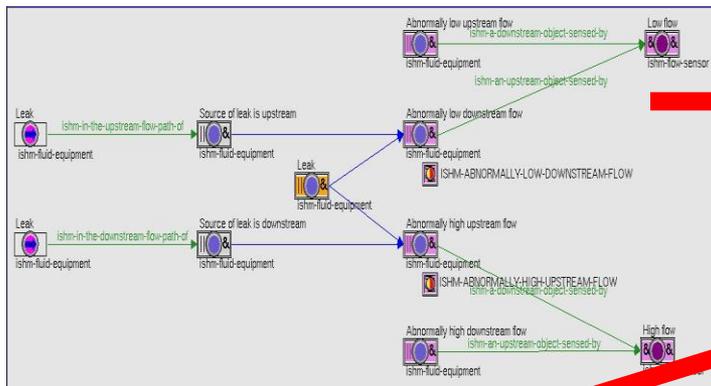
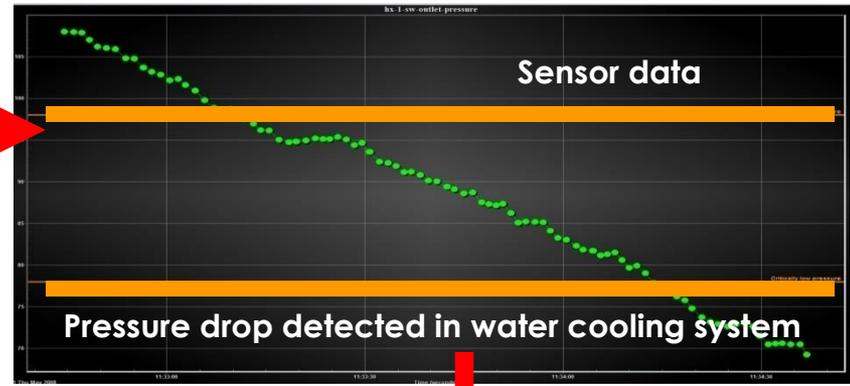
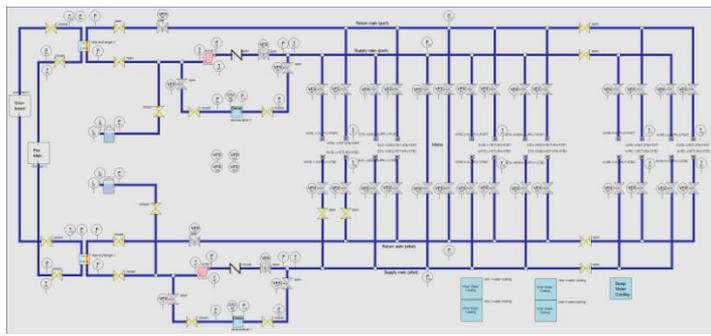
# Fault Detection, Diagnosis, and Prognosis





# Model based reasoning: event detection and diagnosis

Domain model used to predict expected values



Context-specific causal model used for diagnosis

Valve leak

Low pressure downstream of leak

Degraded cooling

Degraded system

# Debugging Specific Fault Models

**Debug Specific Fault Models: Sequential Mode**

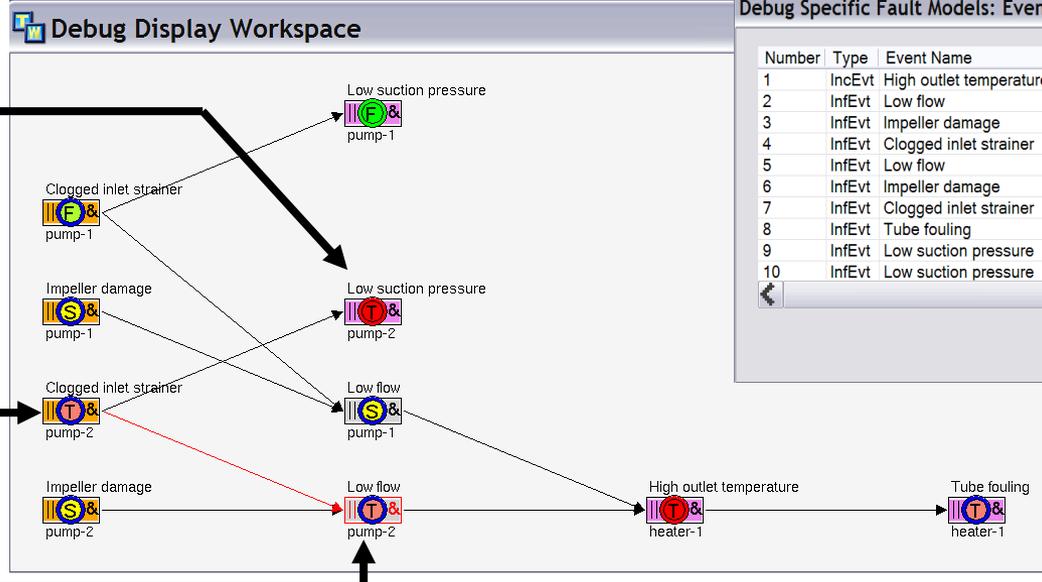
Type	Event Name	Target Object
CurrEvt	Low flow	pump-2
PrevEvt	Clogged inlet strainer	pump-2
IncEvt	Low suction pressure	pump-2

Debug Status: INFER-EVENT      Steps Left: 6      Mode: Sequential

Start At: High outlet temperature::heater-1::true::3/4/2007 22:56:02

Buttons: Advance, Jump, Next, Back

Buttons: Event Log, View Event, View Graph, Graph Options, Close



**Debug Specific Fault Models: Event Log**

Number	Type	Event Name	Target Object	Value	Status	Time Stamp
1	IncEvt	High outlet temperature	heater-1	true	specified	3/4/2007 22:56:02
2	InfEvt	Low flow	pump-2	suspect	upstream inferred	3/4/2007 22:56:02
3	InfEvt	Impeller damage	pump-2	suspect	upstream inferred	3/4/2007 22:56:02
4	InfEvt	Clogged inlet strainer	pump-2	suspect	upstream inferred	3/4/2007 22:56:02
5	InfEvt	Low flow	pump-1	suspect	upstream inferred	3/4/2007 22:56:02
6	InfEvt	Impeller damage	pump-1	suspect	upstream inferred	3/4/2007 22:56:02
7	InfEvt	Clogged inlet strainer	pump-1	suspect	upstream inferred	3/4/2007 22:56:02
8	InfEvt	Tube fouling	heater-1	true	downstream inferred	3/4/2007 22:56:02
9	InfEvt	Low suction pressure	pump-2	suspect	downstream inferred	3/4/2007 22:56:02
10	InfEvt	Low suction pressure	pump-1	suspect	downstream inferred	3/4/2007 22:56:02

Close