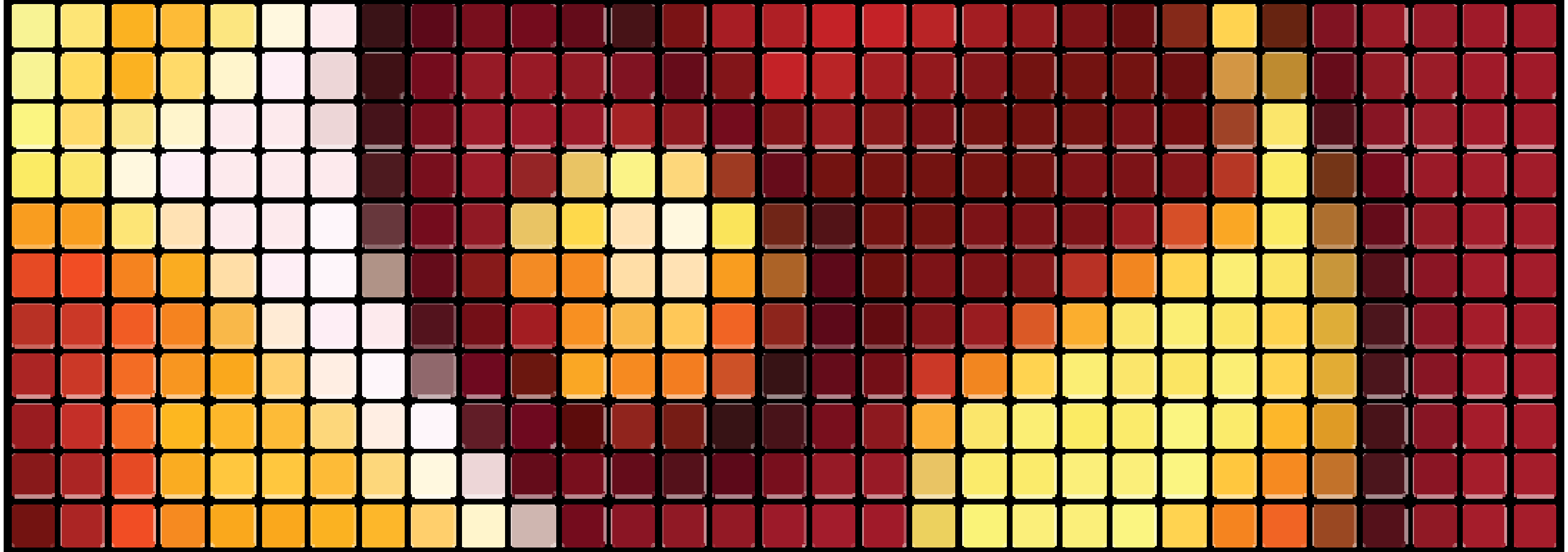
Integration of Model-Based Diagnosis Techniques into the Product Development Chain

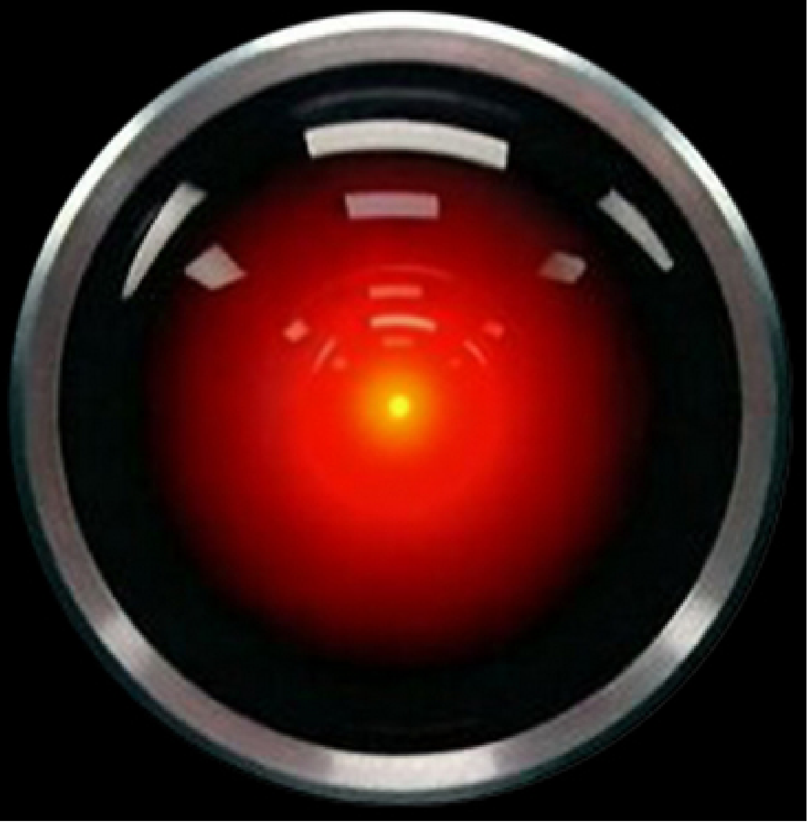


Peter Bunus,

Uptime Solutions AB, Sweden

peter.bunus@uptimeworld.com

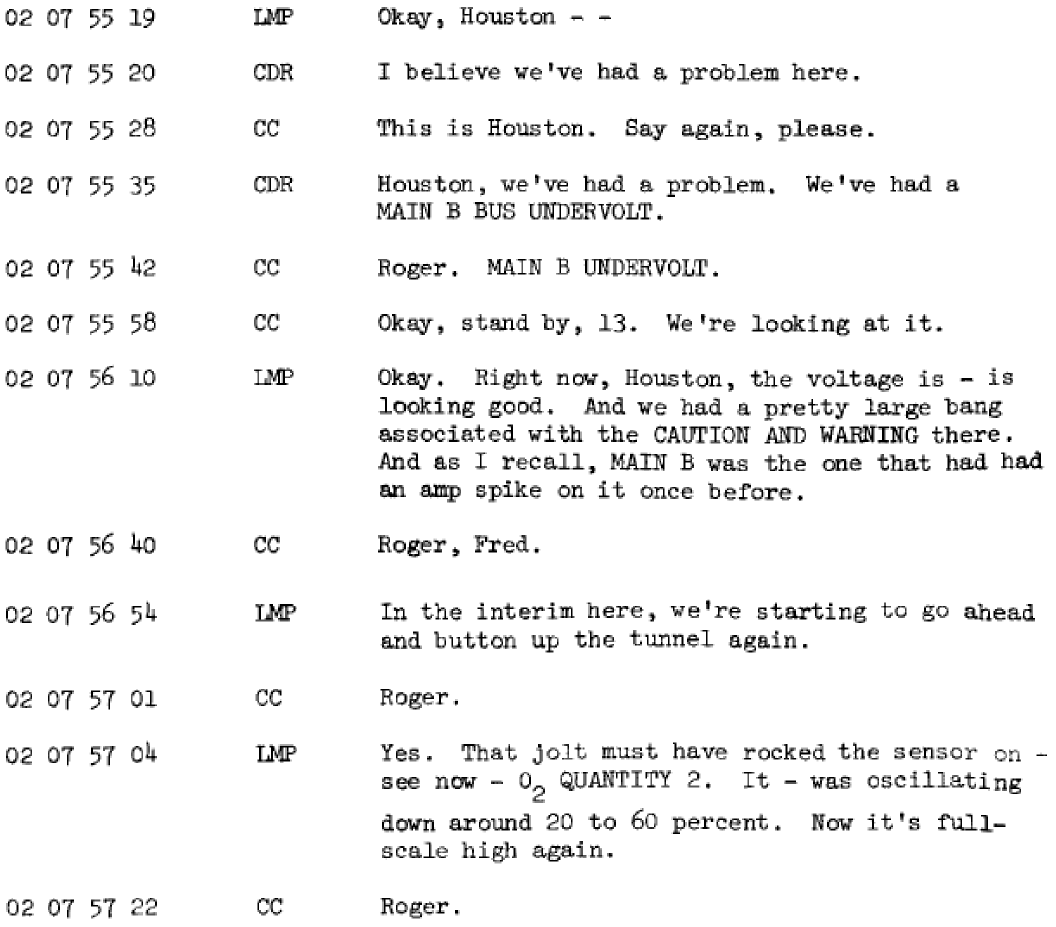
The Diagnostics Problem



“Well HAL, I’m damned if I can find anything wrong with it.”
“Yes. It’s puzzling, isn’t it.”

-- *2001: A Space Odyssey*

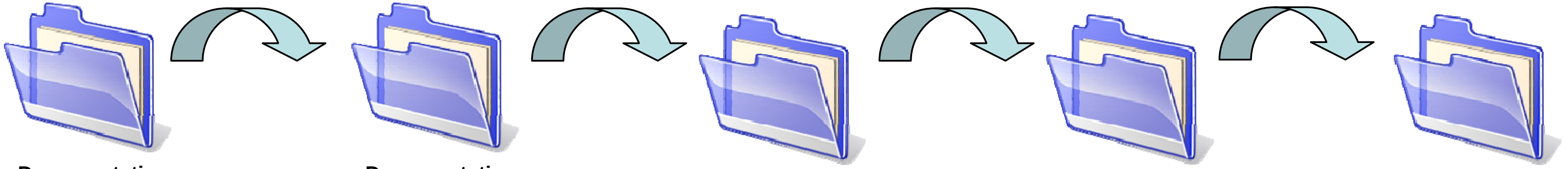
Houston We Have a Problem



02 07 55 19	LMP	Okay, Houston - -
02 07 55 20	CDR	I believe we've had a problem here.
02 07 55 28	CC	This is Houston. Say again, please.
02 07 55 35	CDR	Houston, we've had a problem. We've had a MAIN B BUS UNDERVOLT.
02 07 55 42	CC	Roger. MAIN B UNDERVOLT.
02 07 55 58	CC	Okay, stand by, 13. We're looking at it.
02 07 56 10	LMP	Okay. Right now, Houston, the voltage is - is looking good. And we had a pretty large bang associated with the CAUTION AND WARNING there. And as I recall, MAIN B was the one that had had an amp spike on it once before.
02 07 56 40	CC	Roger, Fred.
02 07 56 54	LMP	In the interim here, we're starting to go ahead and button up the tunnel again.
02 07 57 01	CC	Roger.
02 07 57 04	LMP	Yes. That jolt must have rocked the sensor on - see now - O_2 QUANTITY 2. It - was oscillating down around 20 to 60 percent. Now it's full-scale high again.
02 07 57 22	CC	Roger.

Traditional Design Flow

- Traditional Design Flow
  - Characterized by a sequential flow, iteration is expensive
  - Manual code development, paper intensive, error prone, resistant to change
  - Projects get complex to manage by the end of integration process



REQUIREMENTS ANALYSIS — Documentation

DESIGN — Documentation

IMPLEMENTATION — Documentation & Code and Hardware

INTEGRATION & TESTING — Documentation & Testing

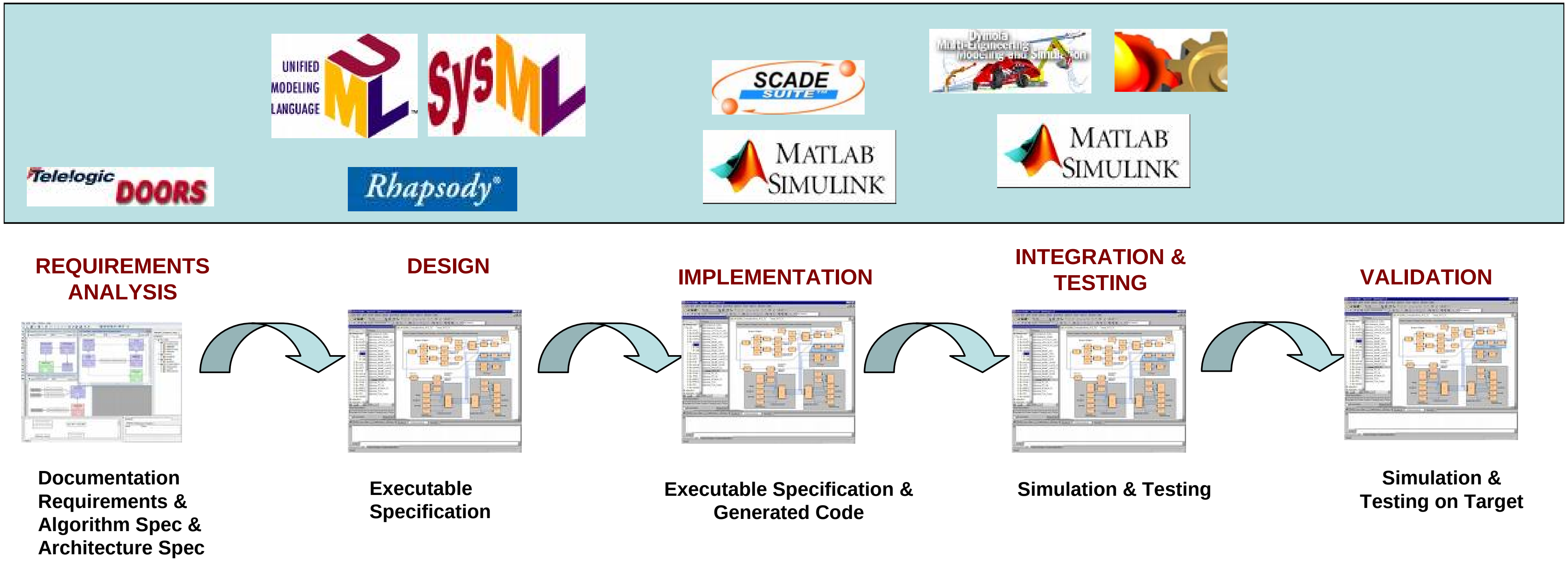
VALIDATION — Documentation & Testing on Target

```
void CruiseControl_init(_C_CruiseControl * _C_)
{
    CruiseSpeedMgt_init(&(_C_->_C0_CruiseSpeedMgt));
    CruiseStateMgt_init(&(_C_->_C3_CruiseStateMgt));
    (_C_->_M_condact_0) = true;
    ThrottleCmd_init(&(_C_->_C4_ThrottleCmd));
    (_C_->_M_init) = true;
}

/* ========= */
/* MAIN NODE */
/* ========= */

void CruiseControl(_C_CruiseControl * _C_)
{
    bool BrakePressed;
    bool AcceleratorPressed;
    bool SpeedOutOffLimits;
    bool _L19;
/*#code for node CruiseControl */
/* call to node not expanded DetectPedalsPressed */
    (_C_->_On_DetectPedalsPressed._I0_Brake) = (_C_->_I
    (_C_->_On_DetectPedalsPressed._I1_Accelerator) = (_
    DetectPedalsPressed(&(_C_->_On_DetectPedalsPressed
    BrakePressed = (_C_->_On_DetectPedalsPressed._O0_B
    AcceleratorPressed =
        (_C_->_On_DetectPedalsPressed._O1_Accelerator
/* call to node not expanded DetectSpeedLimits */
    (_C_->_On_DetectSpeedLimits._I0_speed) = (_C_->_I0_
    DetectSpeedLimits(&(_C_->_On_DetectSpeedLimits));
    SpeedOutOffLimits = (_C_->_On_DetectSpeedLimits._O
/* call to node not expanded CruiseStateMgt */
```

Model-Based Design


Telelogic DOORS
UNIFIED MODELING LANGUAGE UML
SysML
Rhapsody
SCADE SUITE
MATLAB SIMULINK
Dymola Multi-Engineering Modeling and Simulation
MATLAB SIMULINK

REQUIREMENTS ANALYSIS

Documentation
Requirements &
Algorithm Spec &
Architecture Spec

DESIGN

Executable
Specification

IMPLEMENTATION

Executable Specification &
Generated Code

INTEGRATION & TESTING

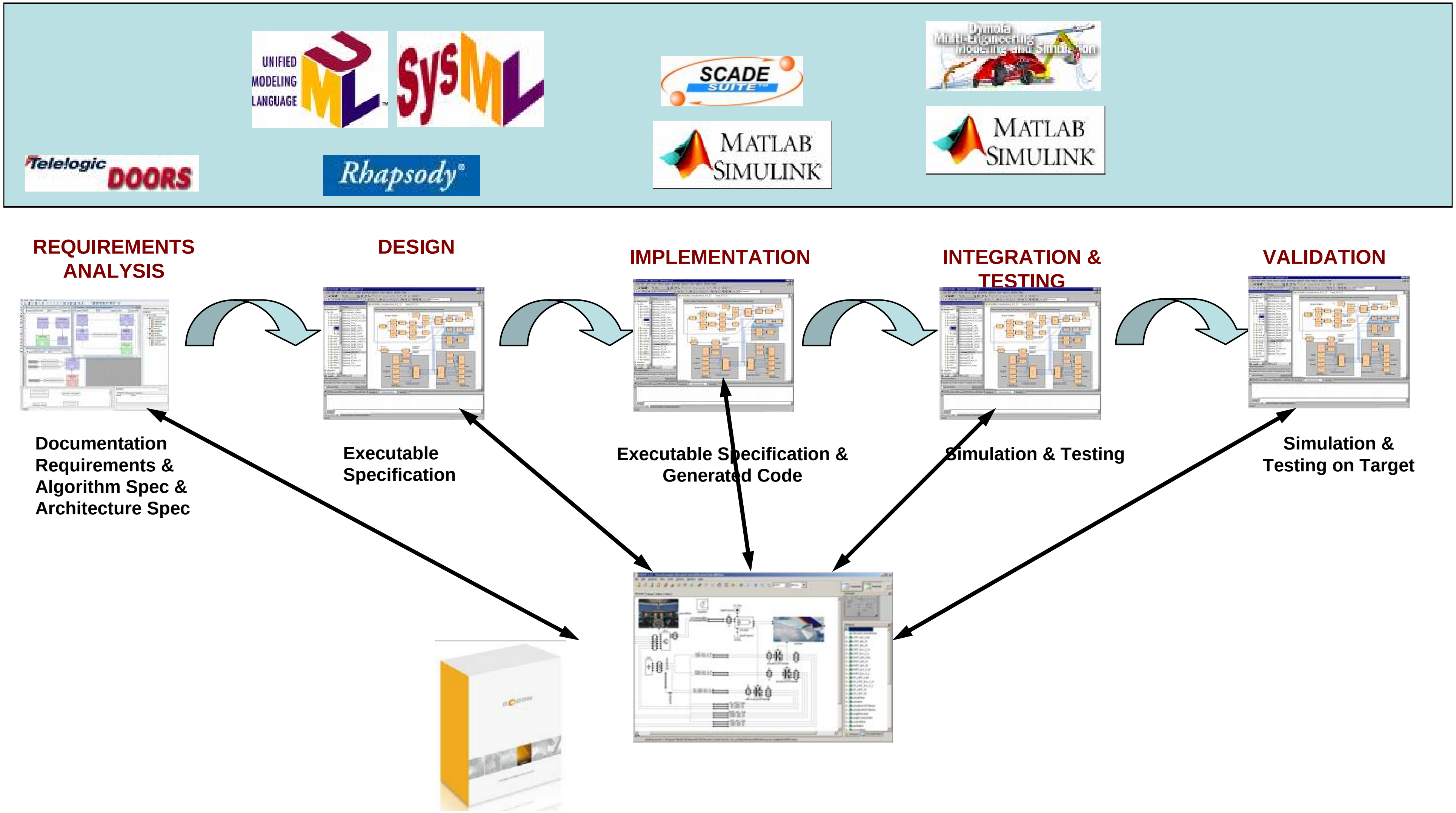
Simulation & Testing

VALIDATION

Simulation &
Testing on Target

- Model-Based Design Flow
  - Build explicit architectures of predictable systems
  - Go seamlessly from abstraction to realizations
  - Capitalize on V& activities early and all along the development flow

Model Driven Development Process


Telelogic DOORS
UNIFIED MODELING LANGUAGE UML
SysML
Rhapsody
SCADE SUITE
MATLAB SIMULINK
Dymola Multi-Engineering Modeling and Simulation
MATLAB SIMULINK

REQUIREMENTS ANALYSIS

DESIGN

IMPLEMENTATION

INTEGRATION & TESTING

VALIDATION

Documentation Requirements & Algorithm Spec & Architecture Spec

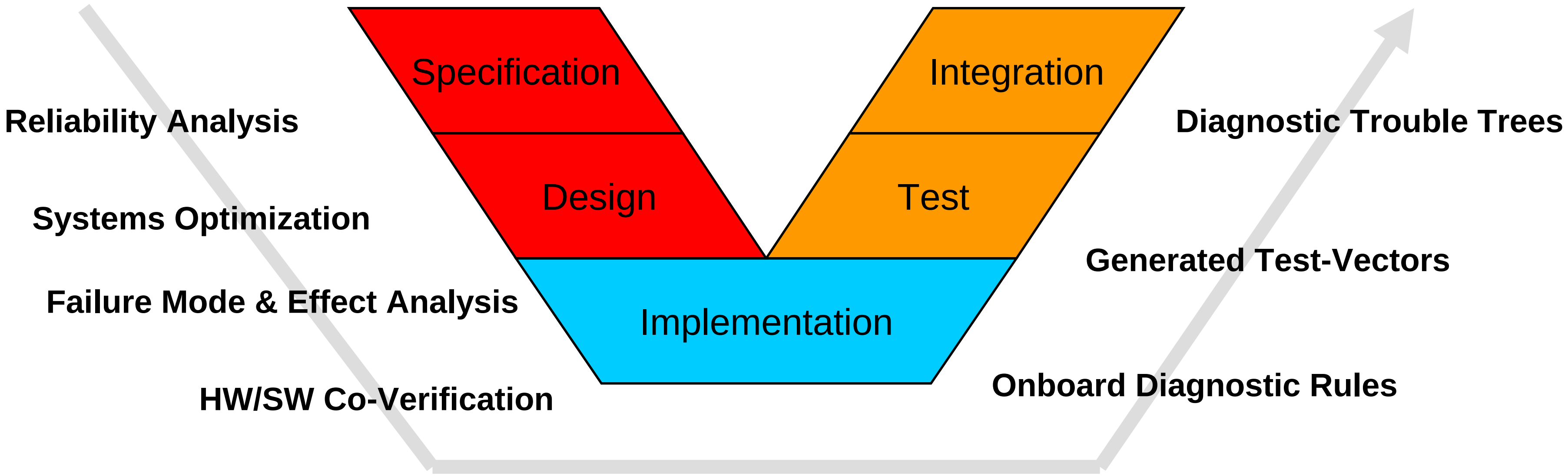
Executable Specification

Executable Specification & Generated Code

Simulation & Testing

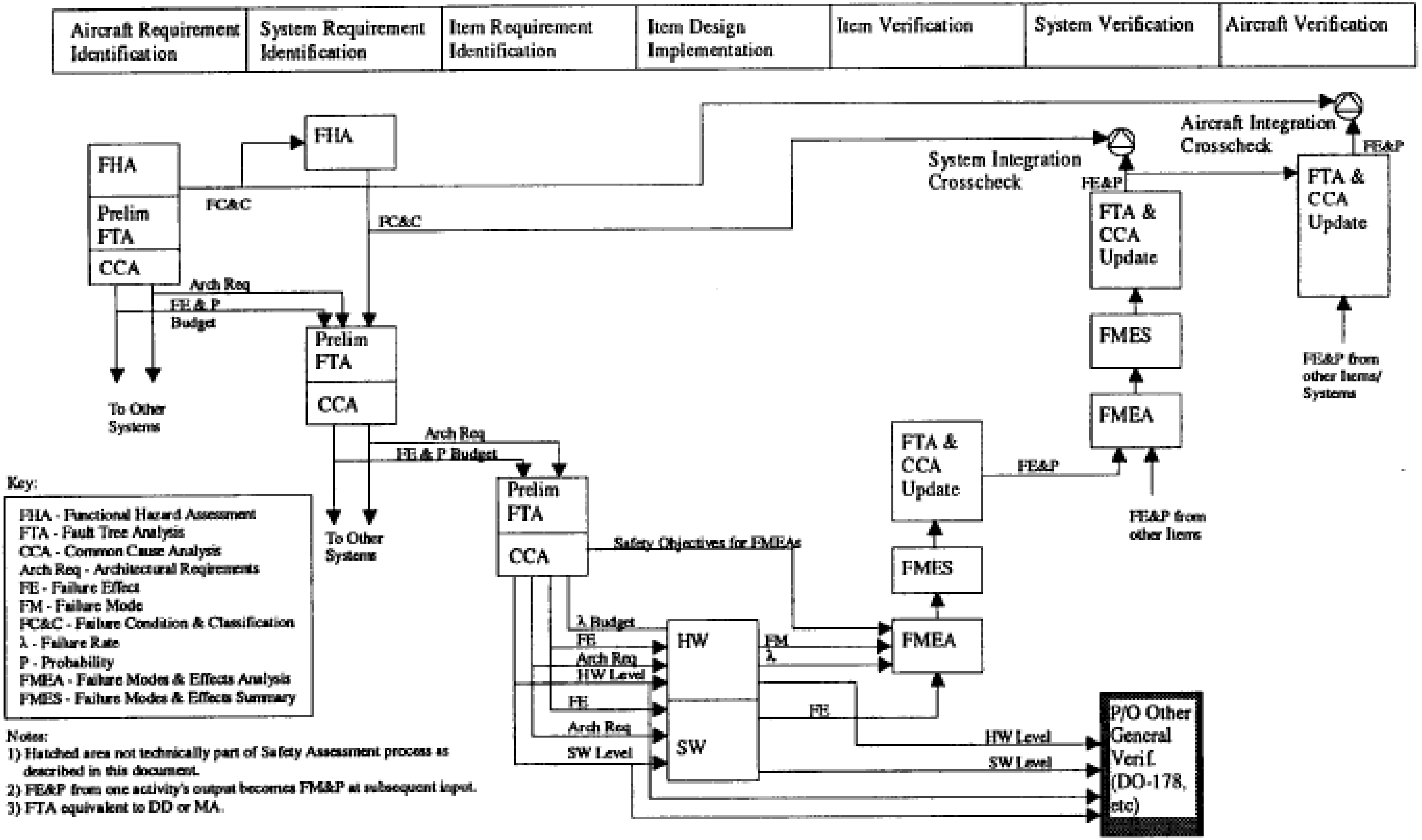
Simulation & Testing on Target

Value of Failure Mode Modeling for the Life Cycle



- Adds value throughout the development cycle
- Executable specification fosters collaboration between departments and organizations
- Provides the missing link between development & service community

ARP 4761 Safety Assessment Diagram



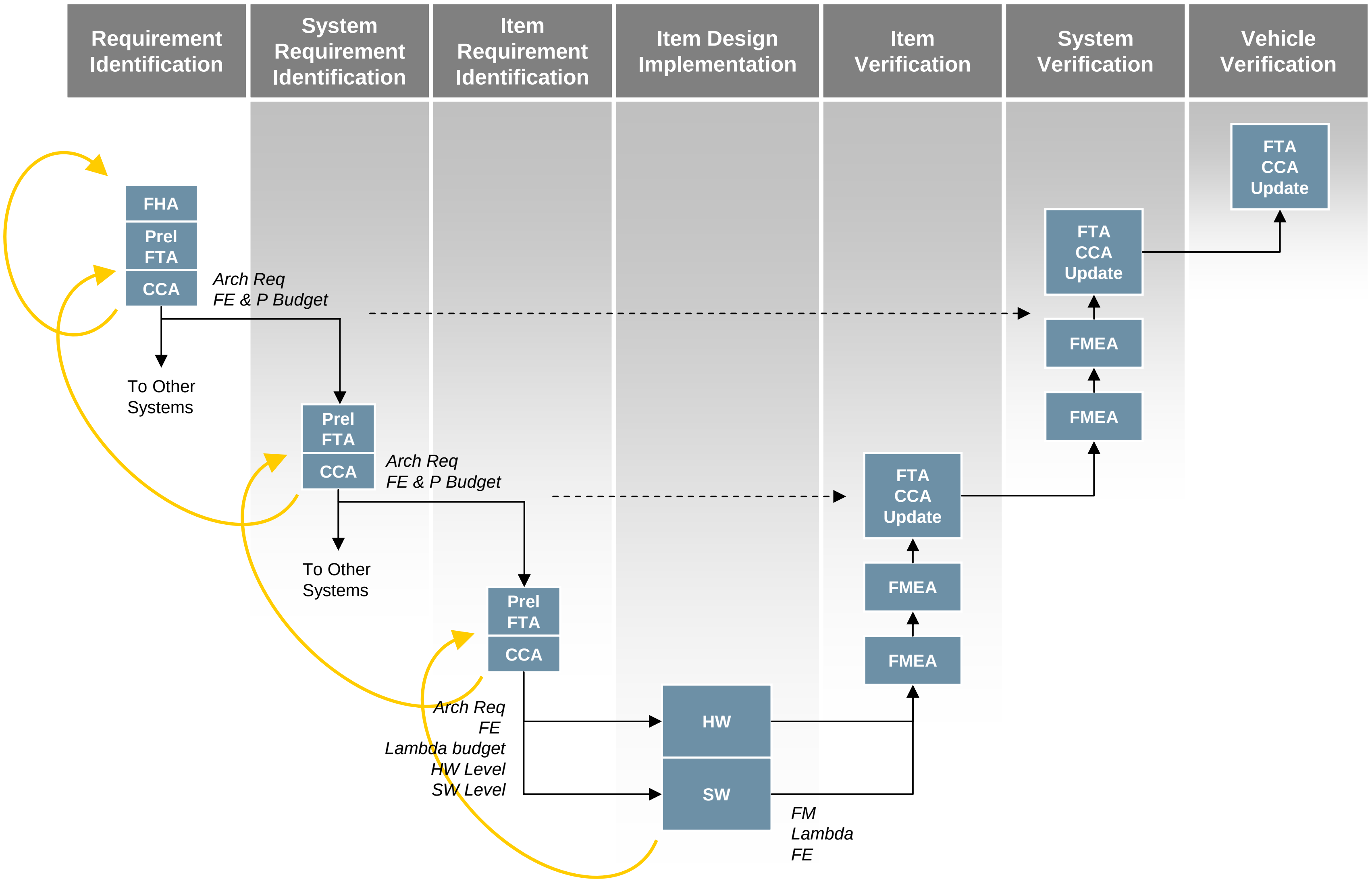
Key:

FHA - Functional Hazard Assessment
FTA - Fault Tree Analysis
CCA - Common Cause Analysis
Arch Req - Architectural Requirements
FE - Failure Effect
FM - Failure Mode
FC&C - Failure Condition & Classification
λ - Failure Rate
P - Probability
FMEA - Failure Modes & Effects Analysis
FMES - Failure Modes & Effects Summary

Notes:

1) Hatched area not technically part of Safety Assessment process as described in this document.
2) FE&P from one activity's output becomes FM&P at subsequent input.
3) FTA equivalent to DD or MA.

ARP 4761 Safety Assessment Diagram



Requirement Identification

System Requirement Identification

Item Requirement Identification

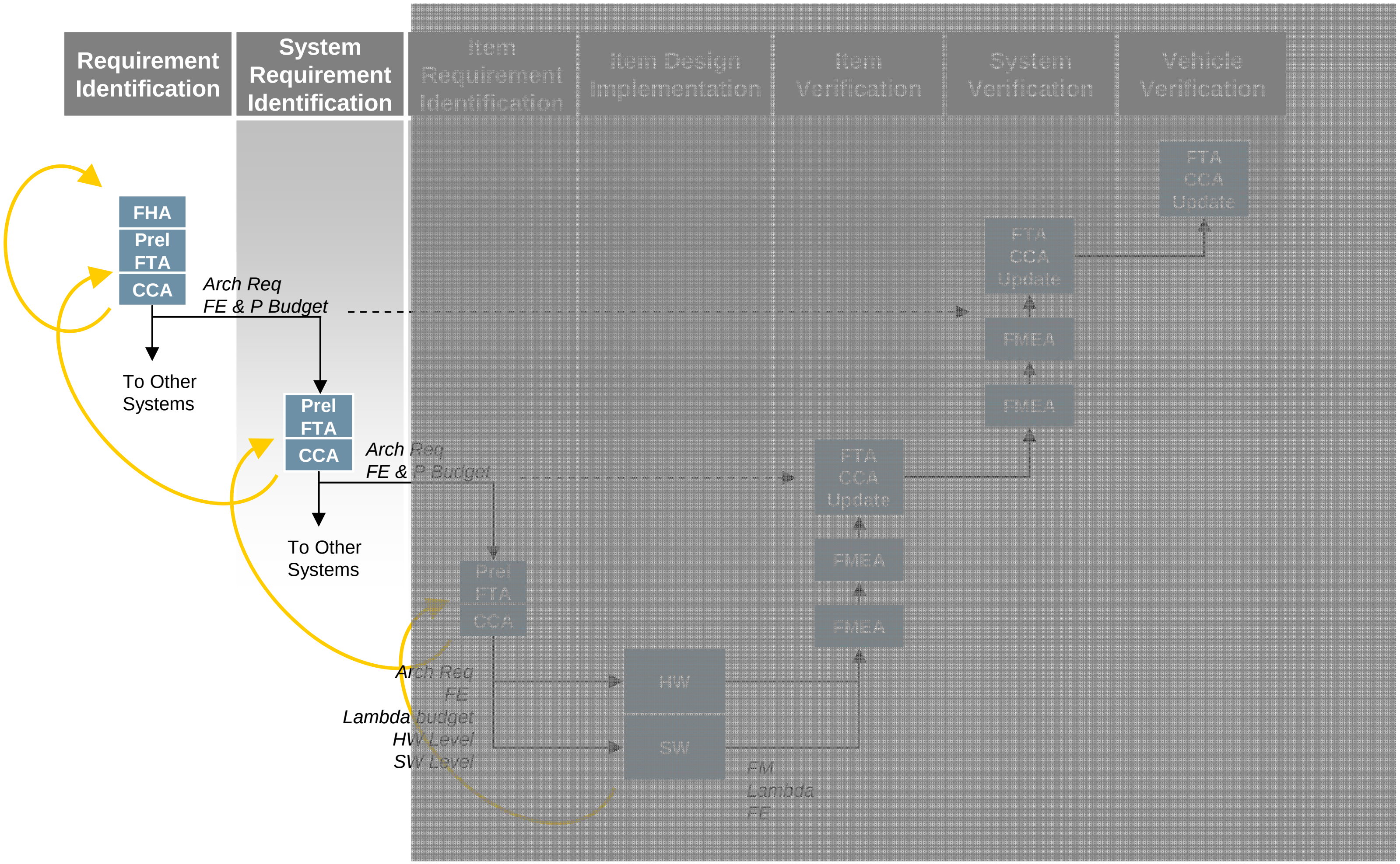
Item Design Implementation

Item Verification

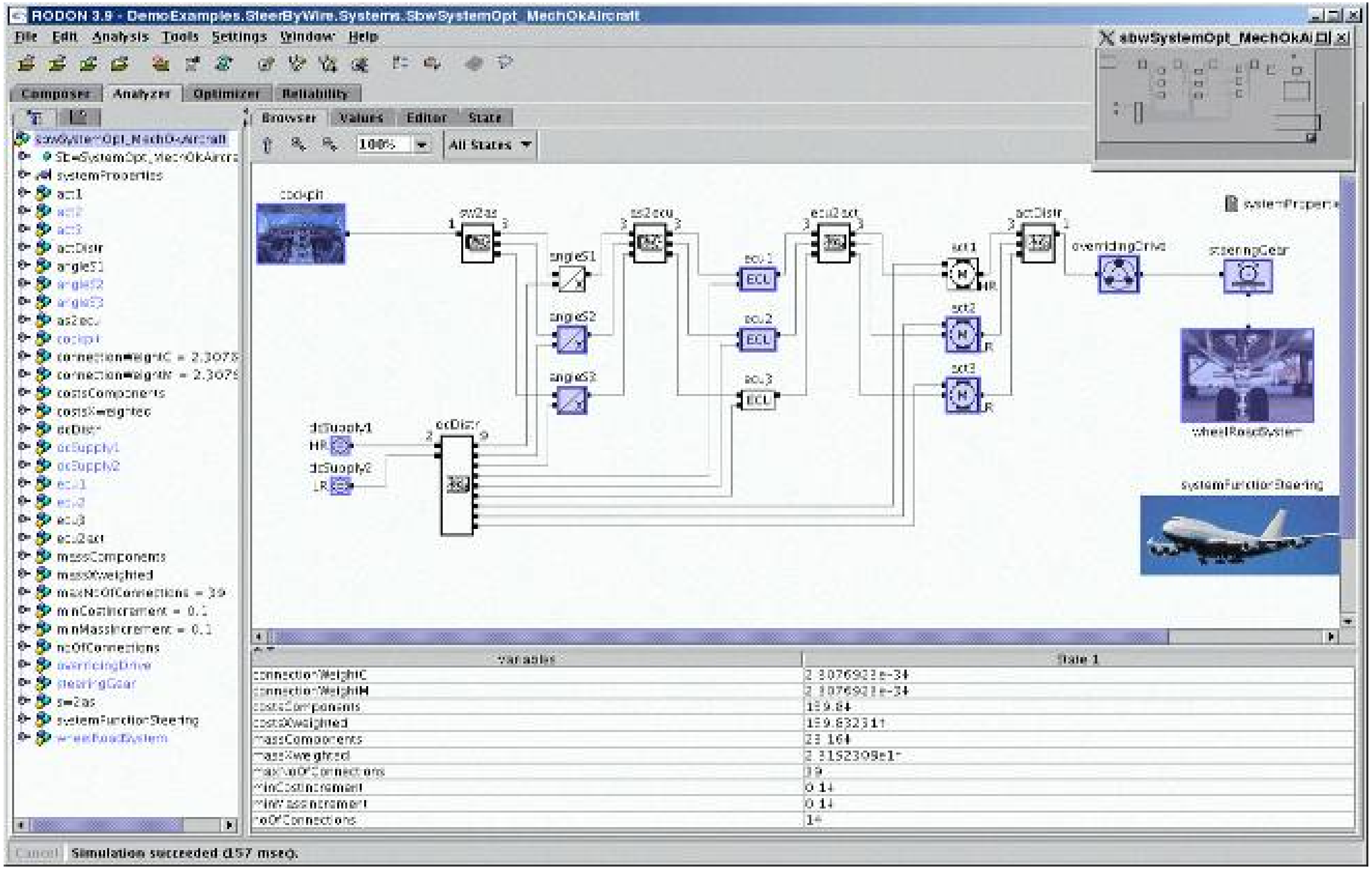
System Verification

Vehicle Verification

Requirements Identification Stage



Models for Quality Insurance



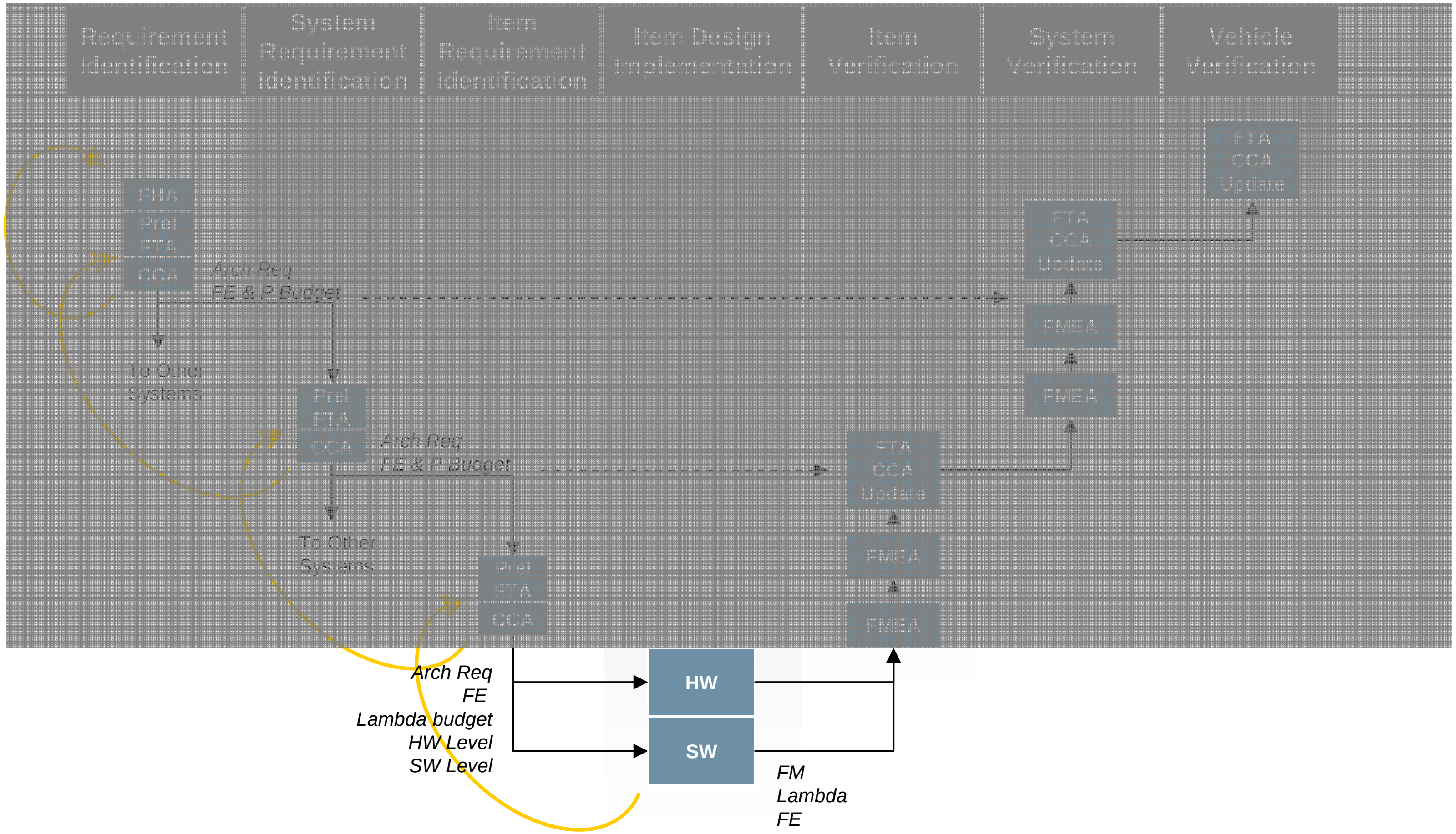
RODON 3.9 - DemoExamples.SteerByWire.Systems.SbwSystemOpt_MechOkAircraft

- sbwSystemOpt_MechOkAircraft
- SbwSystemOpt_MechOkAircra
- systemProperties
- act1
- act2
- act3
- actDistr
- angleS1
- angleS2
- angleS3
- as2ecu
- cockpit
- connectionWeightC = 2.3079
- connectionWeightM = 2.3079
- costsComponents
- costsXweighted
- dcDistr
- dcSupply1
- dcSupply2
- ecu1
- ecu2
- ecu3
- ecu2act
- massComponents
- massXweighted
- maxNoOfConnections = 39
- minCostIncrement = 0.1
- minMassIncrement = 0.1
- noOfConnections
- overridingDrive
- steeringGear
- sw2as
- systemFunctionSteering
- wheelRoadSystem

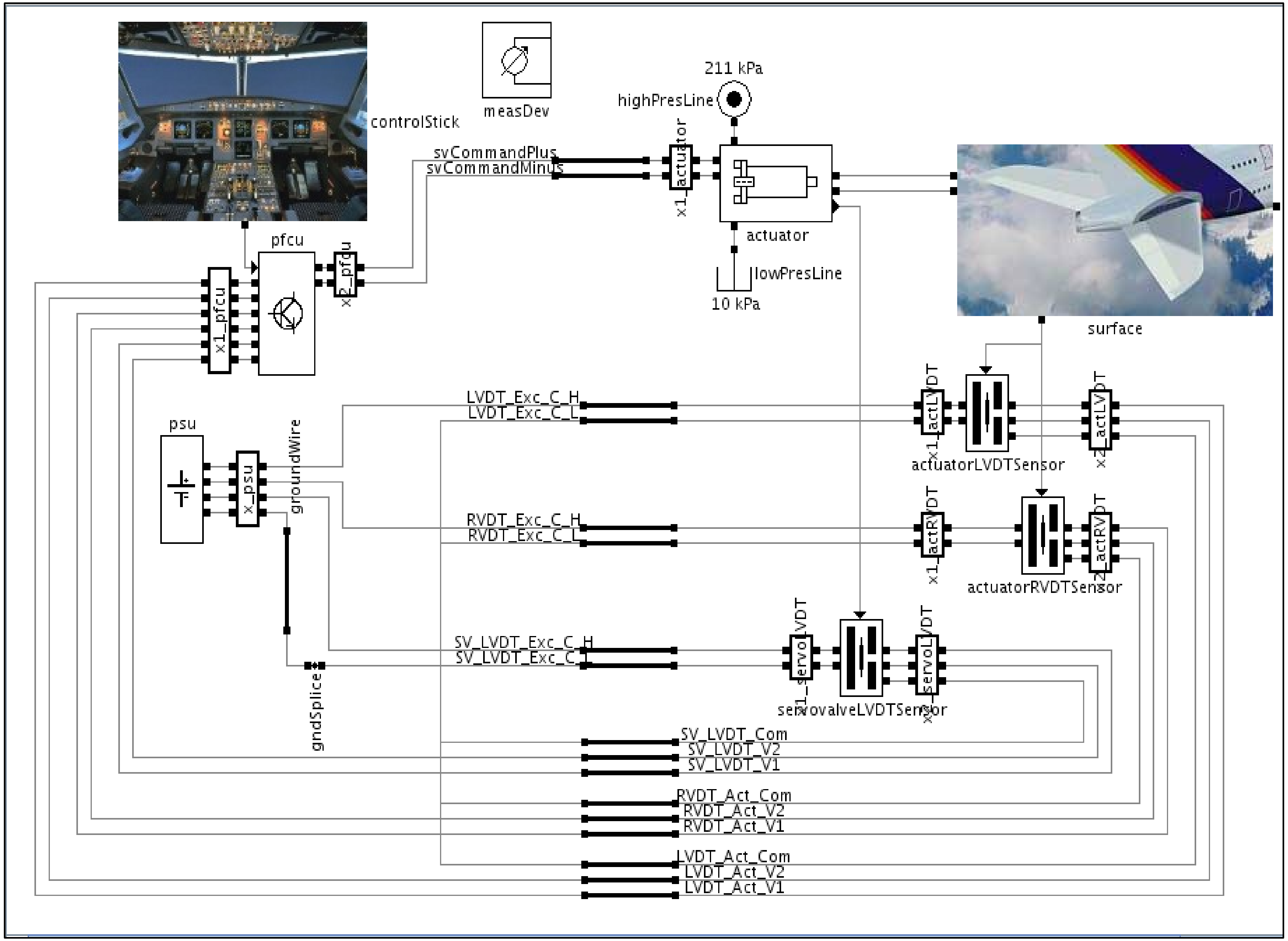
Variables	State 1
connectionWeightC	2.3076923e-34
connectionWeightM	2.3076923e-34
costsComponents	159.84
costsXweighted	159.832311
massComponents	23.164
massXweighted	2.3152309e17
maxNoOfConnections	39
minCostIncrement	0.14
minMassIncrement	0.14
noOfConnections	14

Simulation succeeded (157 msec).

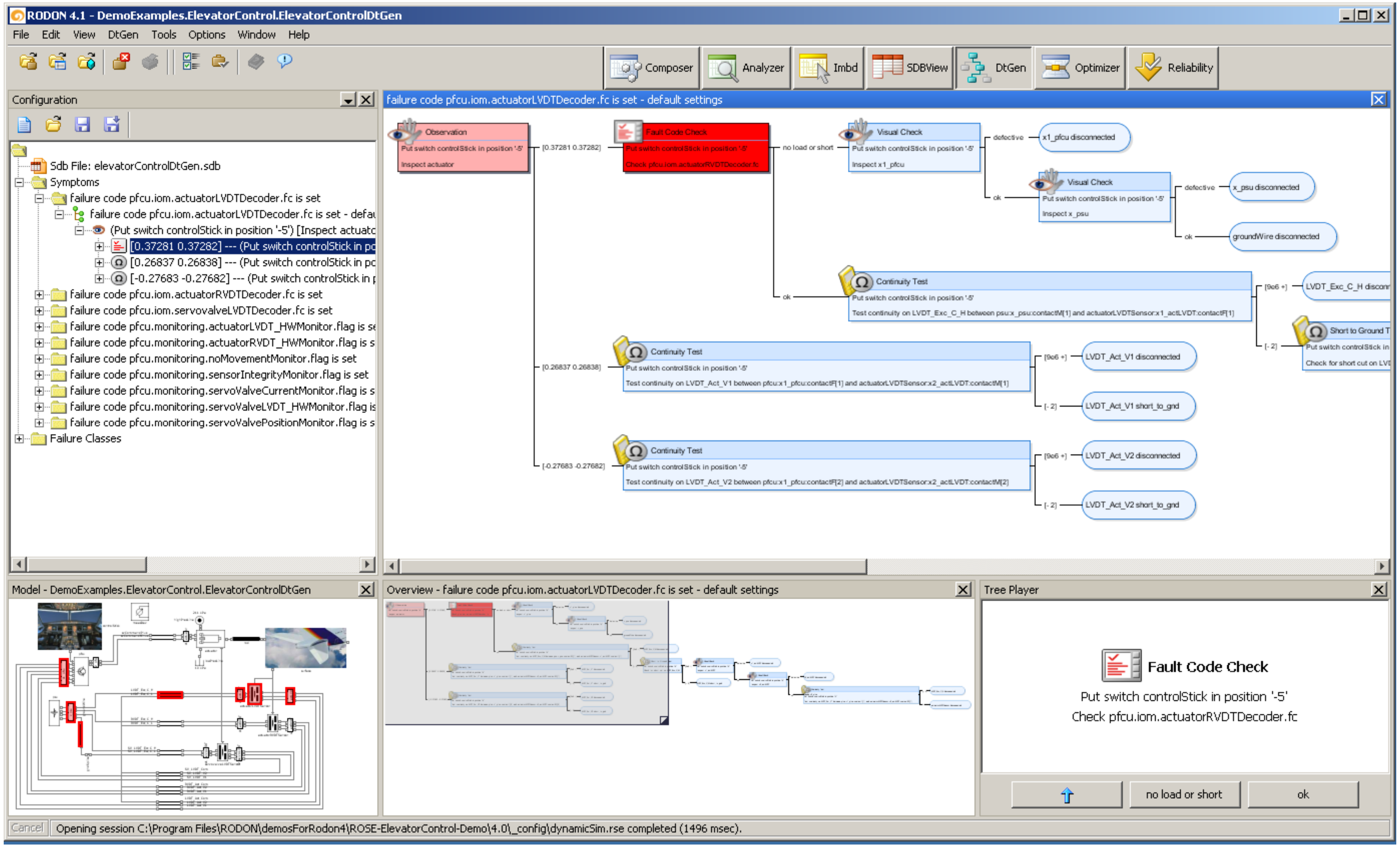
Item Design Implementation Stage



Electronic Elevator Control System



Diagnostics Results – Decision Trees


RODON 4.1 - DemoExamples.ElevatorControl.ElevatorControlDtGen
File
Edit
View
DtGen
Tools
Options
Window
Help
Composer
Analyzer
Imbd
SDBView
DtGen
Optimizer
Reliability
Configuration
Model - DemoExamples.ElevatorControl.ElevatorControlDtGen
Overview - failure code pfcu.iom.actuatorLVDTDecoder.fc is set - default settings
Tree Player
Cancel

Sdb File: elevatorControlDtGen.sdb
Symptoms
failure code pfcu.iom.actuatorLVDTDecoder.fc is set
failure code pfcu.iom.actuatorLVDTDecoder.fc is set - defau
(Put switch controlStick in position '-5') [Inspect actuatc
[0.37281 0.37282] --- (Put switch controlStick in pc
[0.26837 0.26838] --- (Put switch controlStick in pc
[-0.27683 -0.27682] --- (Put switch controlStick in p
failure code pfcu.iom.actuatorRVDTDecoder.fc is set
failure code pfcu.iom.servovalveLVDTDecoder.fc is set
failure code pfcu.monitoring.actuatorLVDT_HWMonitor.flag is se
failure code pfcu.monitoring.actuatorRVDT_HWMonitor.flag is s
failure code pfcu.monitoring.noMovementMonitor.flag is set
failure code pfcu.monitoring.sensorIntegrityMonitor.flag is set
failure code pfcu.monitoring.servoValveCurrentMonitor.flag is s
failure code pfcu.monitoring.servoValveLVDT_HWMonitor.flag is
failure code pfcu.monitoring.servoValvePositionMonitor.flag is s
Failure Classes

failure code pfcu.iom.actuatorLVDTDecoder.fc is set - default settings

Observation
Put switch controlStick in position '-5'
Inspect actuator

[0.37281 0.37282]

Fault Code Check
Put switch controlStick in position '-5'
Check pfcu.iom.actuatorRVDTDecoder.fc

no load or short

Visual Check
Put switch controlStick in position '-5'
Inspect x1_pfcu

defective — x1_pfcu disconnected

ok

Visual Check
Put switch controlStick in position '-5'
Inspect x_psu

defective — x_psu disconnected

ok — groundWire disconnected

ok

Continuity Test
Put switch controlStick in position '-5'
Test continuity on LVDT_Exc_C_H between psu:x_psu:contactM[1] and actuatorLVDTSensor:x1_actLVDT:contactF[1]

[9e6 +] — LVDT_Exc_C_H discon

[- 2]

Short to Ground T
Put switch controlStick in
Check for short cut on LVI

[0.26837 0.26838]

Continuity Test
Put switch controlStick in position '-5'
Test continuity on LVDT_Act_V1 between pfcu:x1_pfcu:contactF[1] and actuatorLVDTSensor:x2_actLVDT:contactM[1]

[9e6 +] — LVDT_Act_V1 disconnected

[- 2] — LVDT_Act_V1 short_to_gnd

[-0.27683 -0.27682]

Continuity Test
Put switch controlStick in position '-5'
Test continuity on LVDT_Act_V2 between pfcu:x1_pfcu:contactF[2] and actuatorLVDTSensor:x2_actLVDT:contactM[2]

[9e6 +] — LVDT_Act_V2 disconnected

[- 2] — LVDT_Act_V2 short_to_gnd

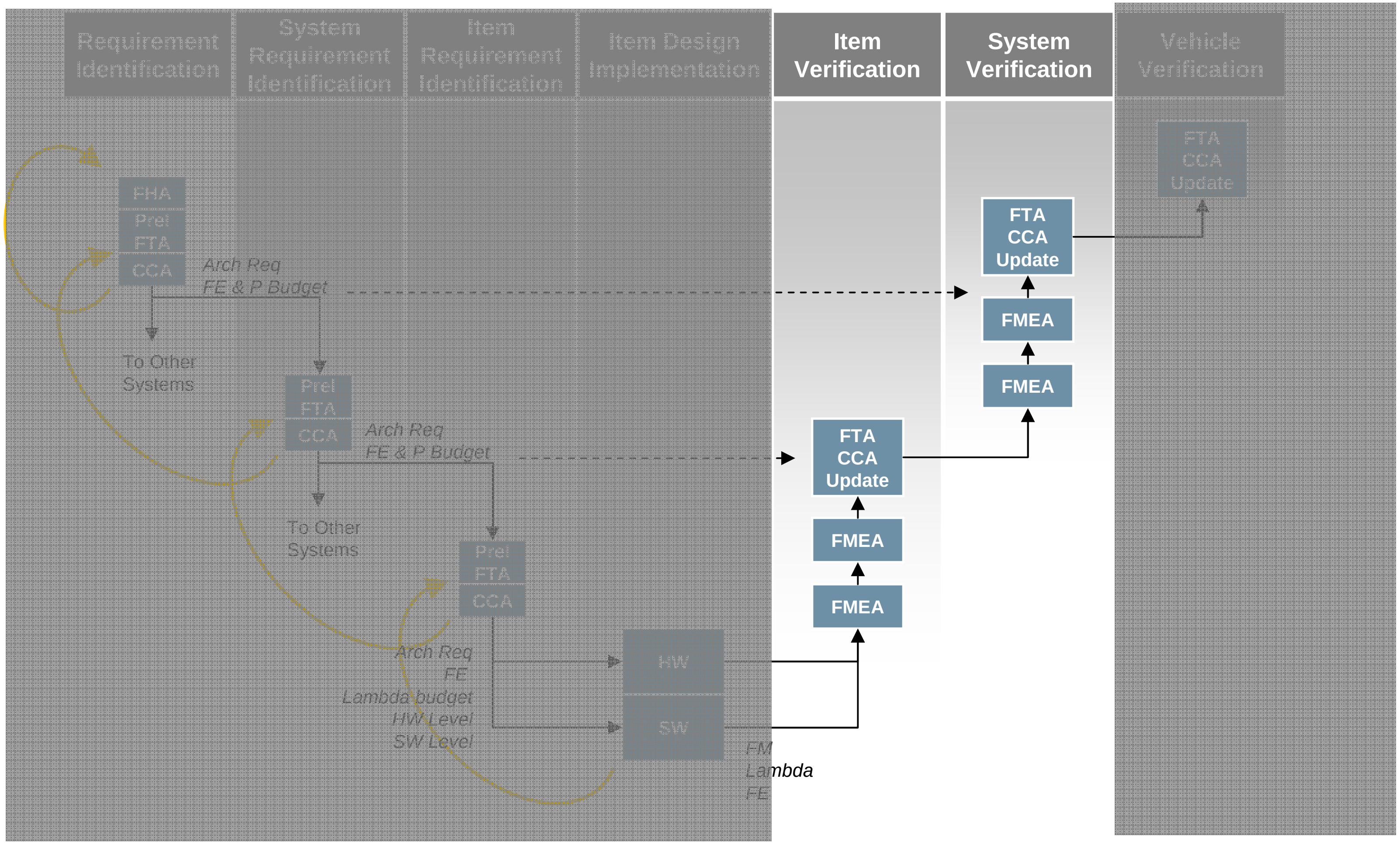
Fault Code Check
Put switch controlStick in position '-5'
Check pfcu.iom.actuatorRVDTDecoder.fc

no load or short

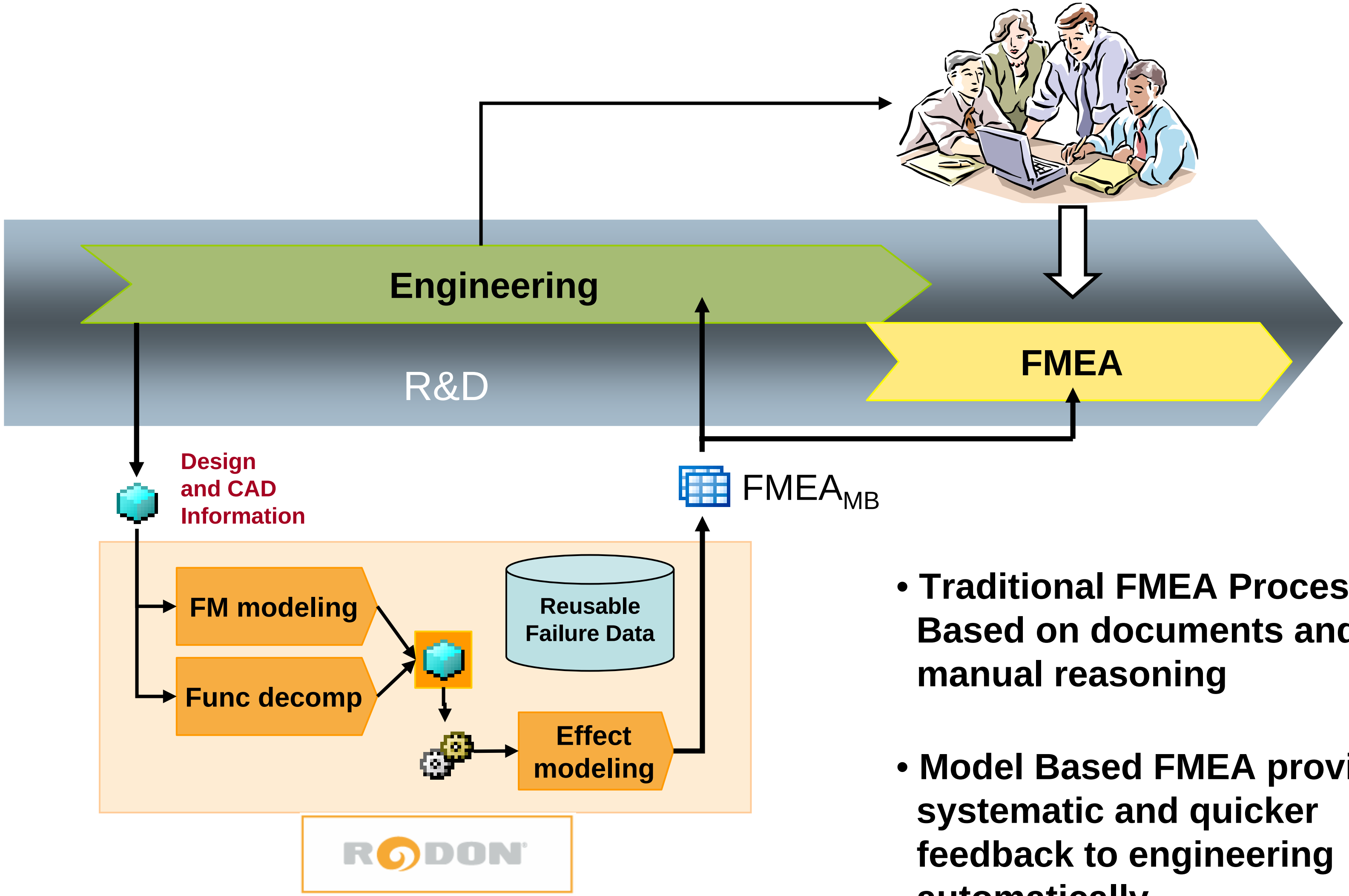
ok

Opening session C:\Program Files\RODON\demosForRodon4\ROSE-ElevatorControl-Demo\4.0_config\dynamicSim.rse completed (1496 msec).

Item & System Verification Stage

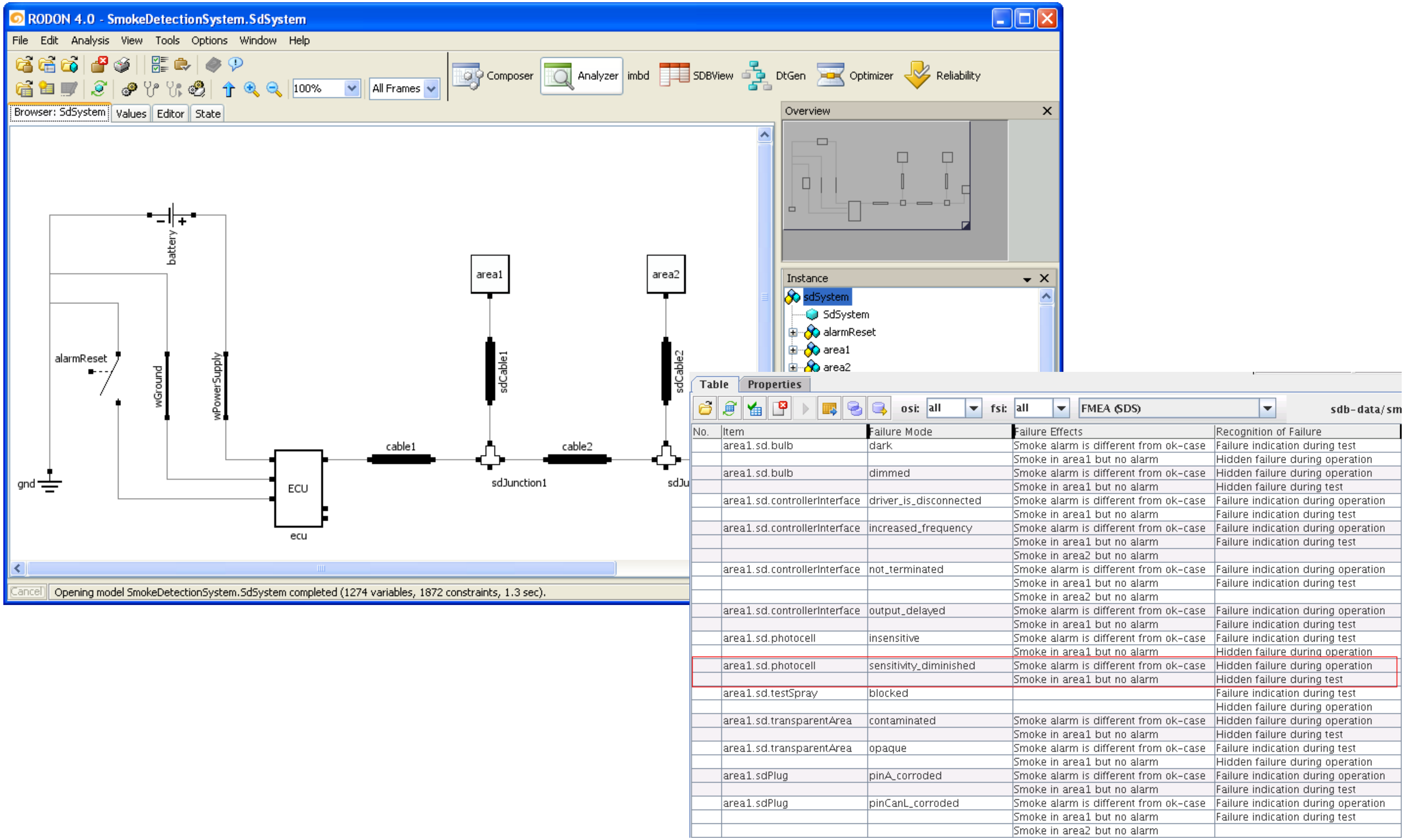


The FMEA Process



- Traditional FMEA Process. Based on documents and manual reasoning
- Model Based FMEA provide systematic and quicker feedback to engineering automatically

Tutorial Demo Model and Generated FMEA



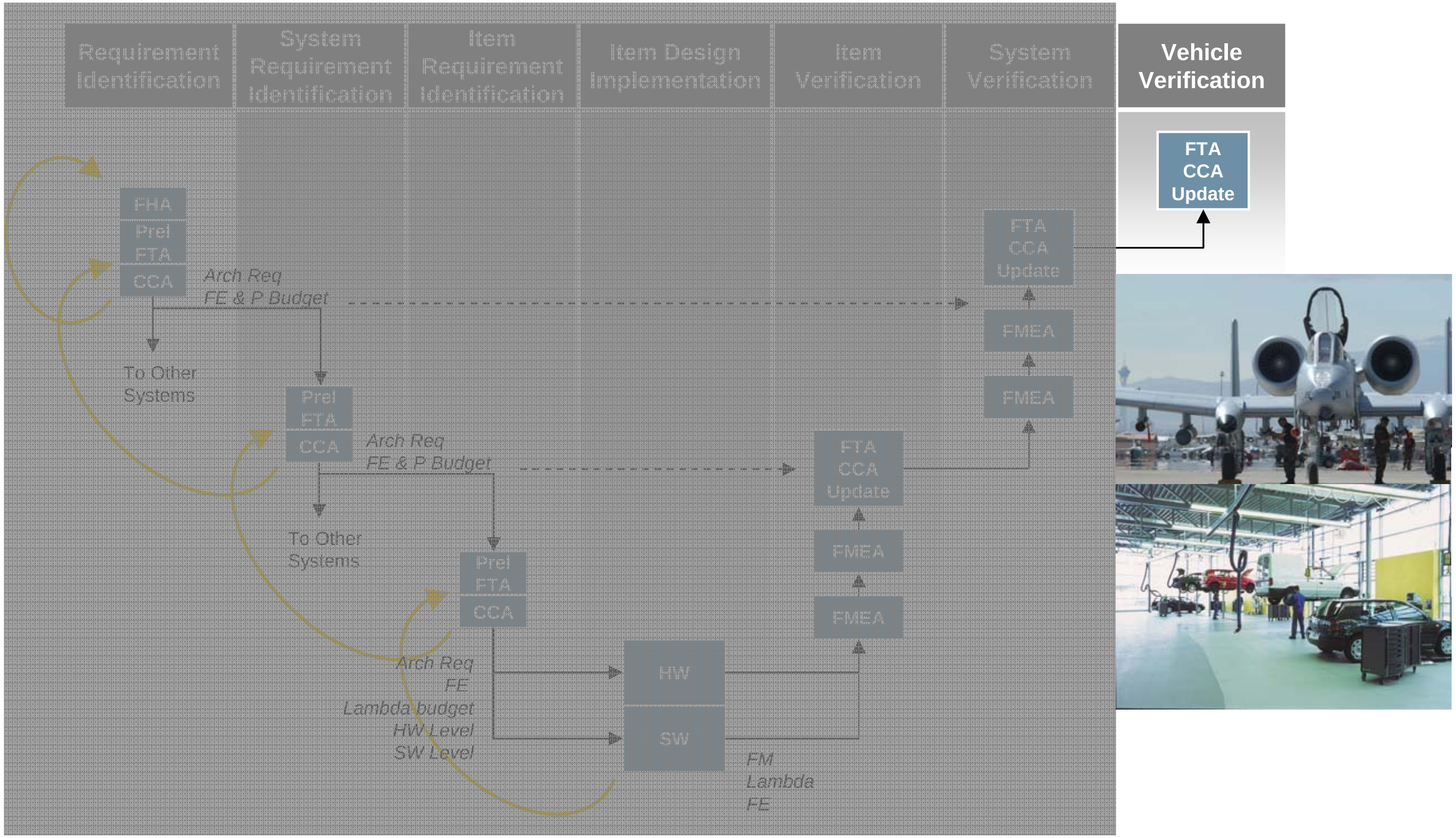
Opening model SmokeDetectionSystem.SdSystem completed (1274 variables, 1872 constraints, 1.3 sec).

osi: all fsi: all FMEA (SDS)

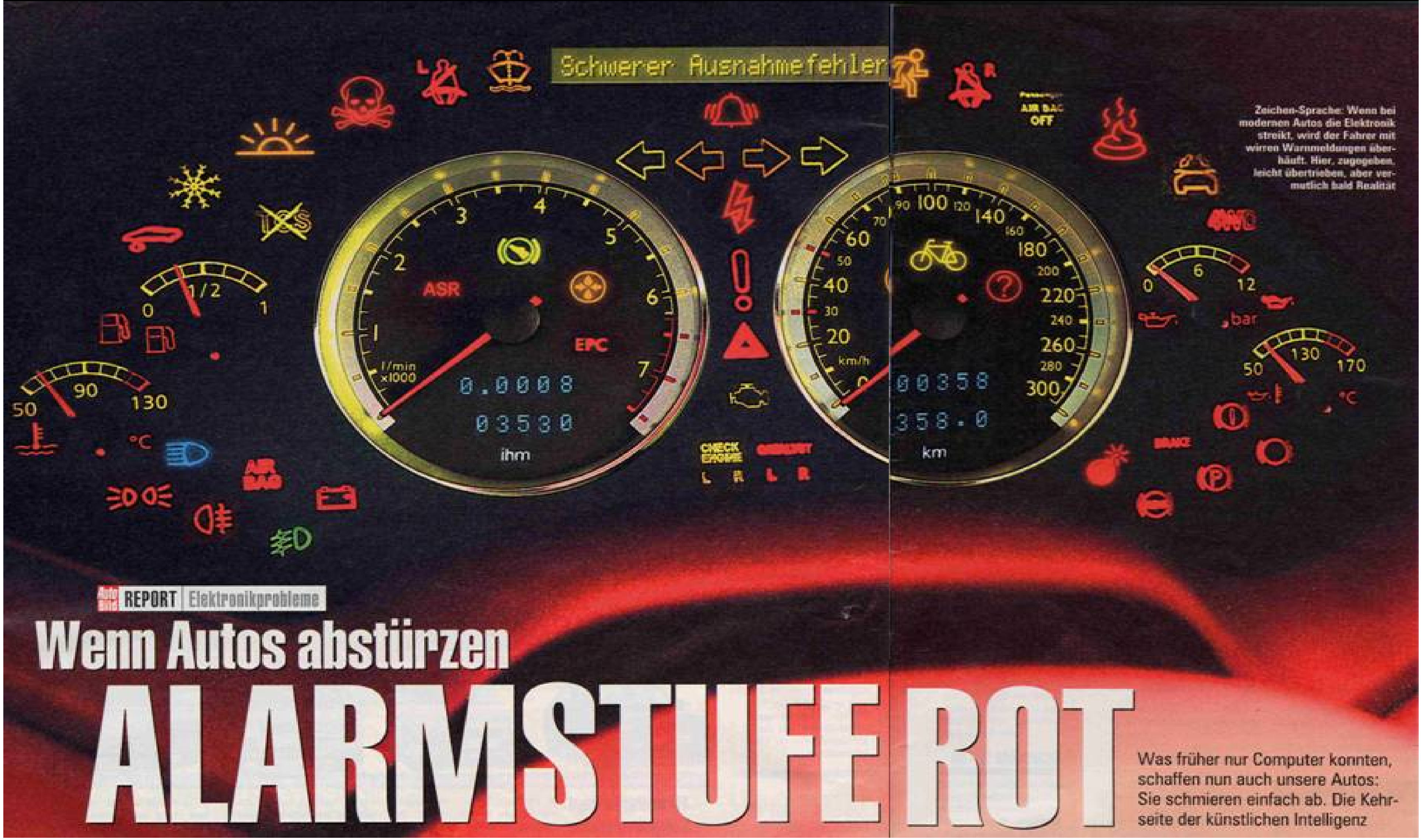
No.	Item	Failure Mode	Failure Effects	Recognition of Failure
	area1.sd.bulb	dark	Smoke alarm is different from ok-case	Failure indication during test
			Smoke in area1 but no alarm	Hidden failure during operation
	area1.sd.bulb	dimmed	Smoke alarm is different from ok-case	Hidden failure during operation
			Smoke in area1 but no alarm	Hidden failure during test
	area1.sd.controllerInterface	driver_is_disconnected	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
	area1.sd.controllerInterface	increased_frequency	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
			Smoke in area2 but no alarm	
	area1.sd.controllerInterface	not_terminated	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
			Smoke in area2 but no alarm	
	area1.sd.controllerInterface	output_delayed	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
	area1.sd.photocell	insensitive	Smoke alarm is different from ok-case	Failure indication during test
			Smoke in area1 but no alarm	Hidden failure during operation
	area1.sd.photocell	sensitivity_diminished	Smoke alarm is different from ok-case	Hidden failure during operation
			Smoke in area1 but no alarm	Hidden failure during test
	area1.sd.testSpray	blocked		Failure indication during test
				Hidden failure during operation
	area1.sd.transparentArea	contaminated	Smoke alarm is different from ok-case	Hidden failure during operation
			Smoke in area1 but no alarm	Hidden failure during test
	area1.sd.transparentArea	opaque	Smoke alarm is different from ok-case	Failure indication during test
			Smoke in area1 but no alarm	Hidden failure during operation
	area1.sdPlug	pinA_corroded	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
	area1.sdPlug	pinCanL_corroded	Smoke alarm is different from ok-case	Failure indication during operation
			Smoke in area1 but no alarm	Failure indication during test
			Smoke in area2 but no alarm	

[redacted]

Vehicle Verification Stage



The Diagnosis Problem



Schwerer Ausnahmefehler
Passenger AIR BAG OFF
ASR
EPC
1/min ×1000
0.0008
03530
ihm
km/h
00358
358.0
km
CHECK ENGINE
L R L R
AIR BAG
BRAKE
bar
°C
1/2

Zeichen-Sprache: Wenn bei modernen Autos die Elektronik streikt, wird der Fahrer mit wirren Warnmeldungen überhäuft. Hier, zugegeben, leicht übertrieben, aber vermutlich bald Realität

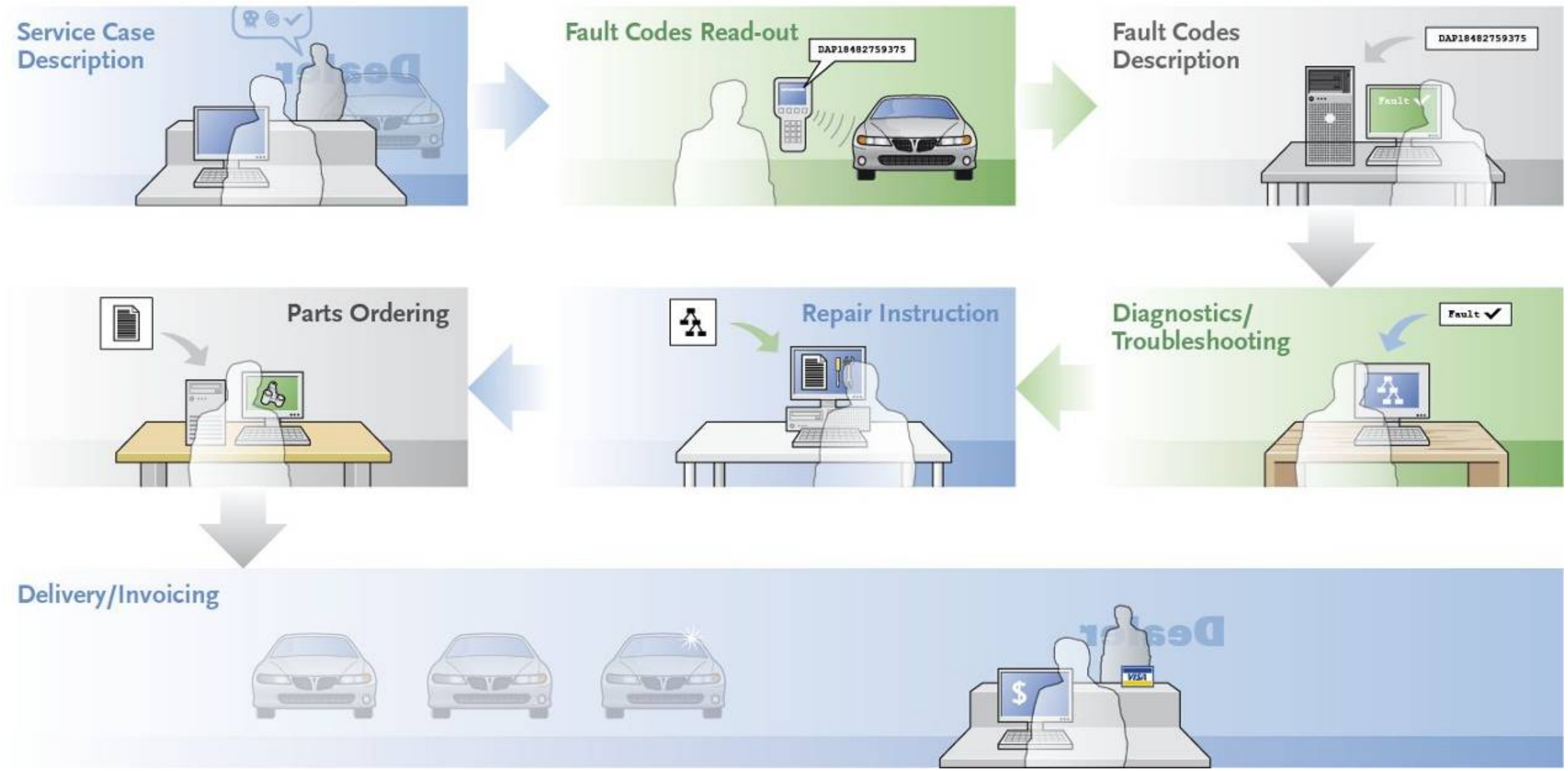
Auto Bild REPORT | Elektronikprobleme

Wenn Autos abstürzen

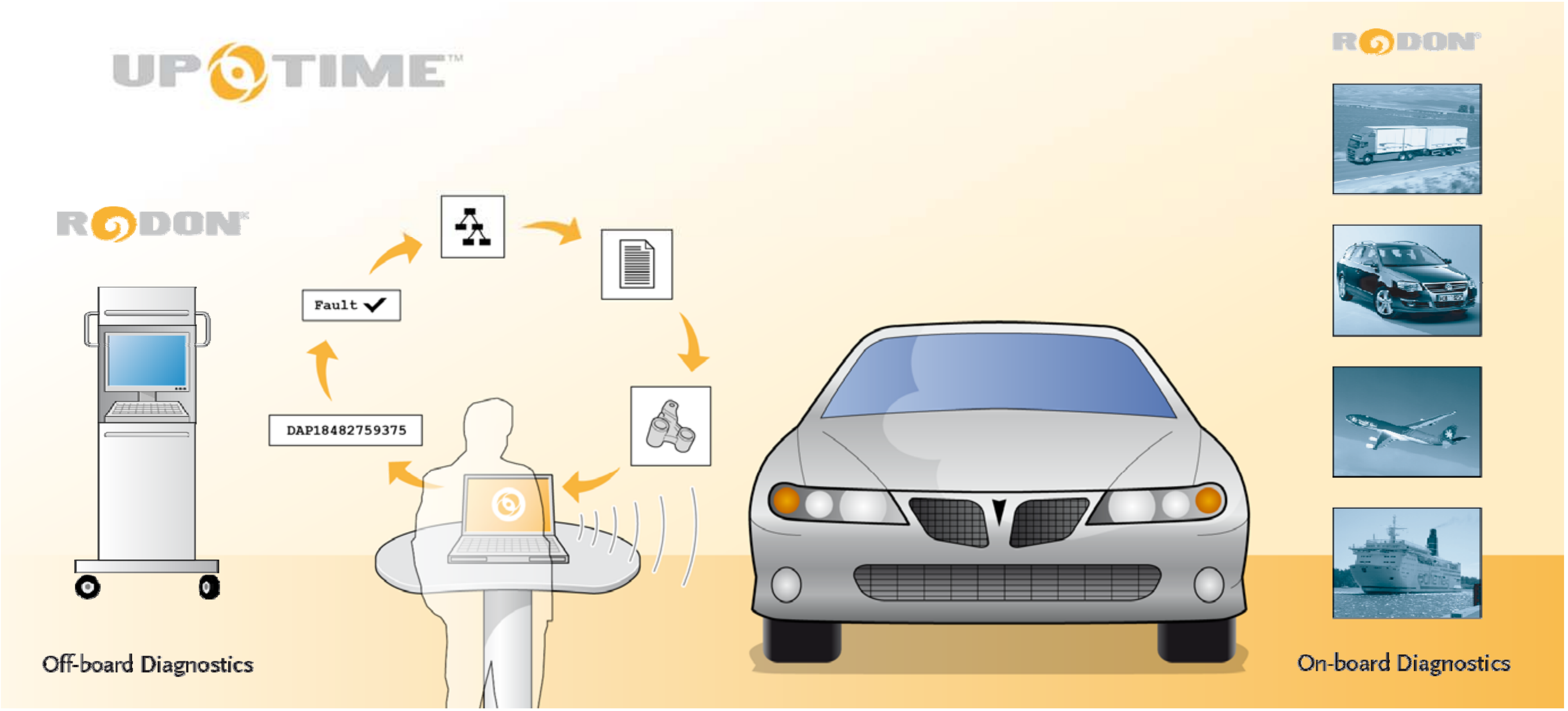
ALARMSTUFE ROT

Was früher nur Computer konnten, schaffen nun auch unsere Autos: Sie schmieren einfach ab. Die Kehrseite der künstlichen Intelligenz

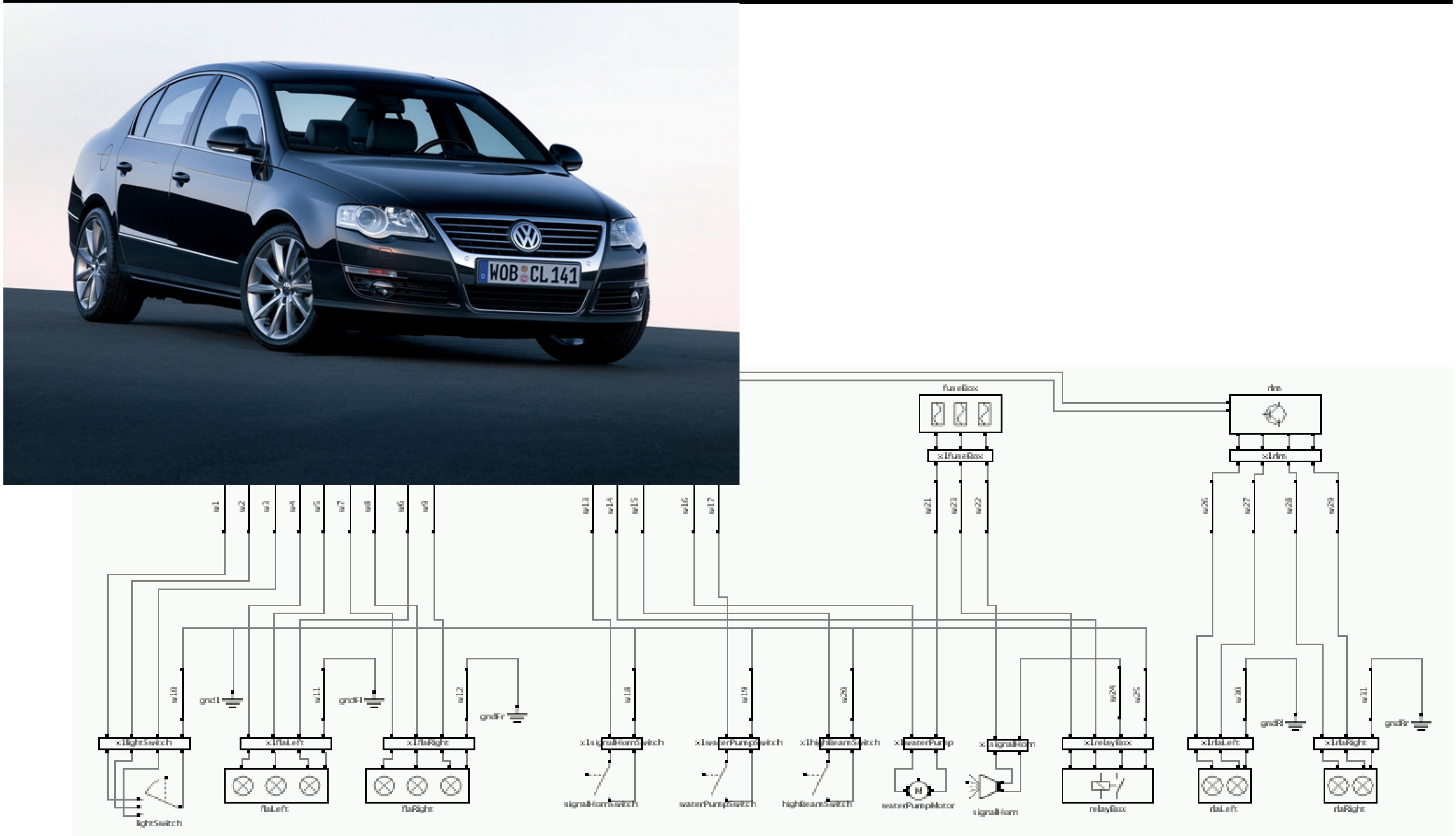
Traditional Service Process



Workshop Off-Board Diagnostics Scenario



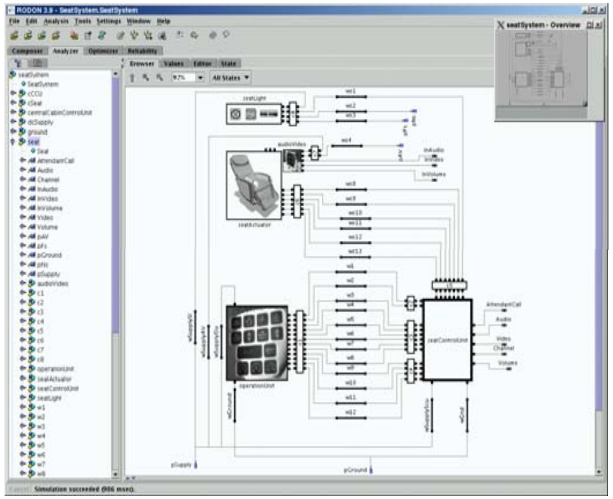
Tutorial Demo Exterior Lighting



Model-Based Diagnosis Principles

Actual system

Observed behavior



Model of the system

design

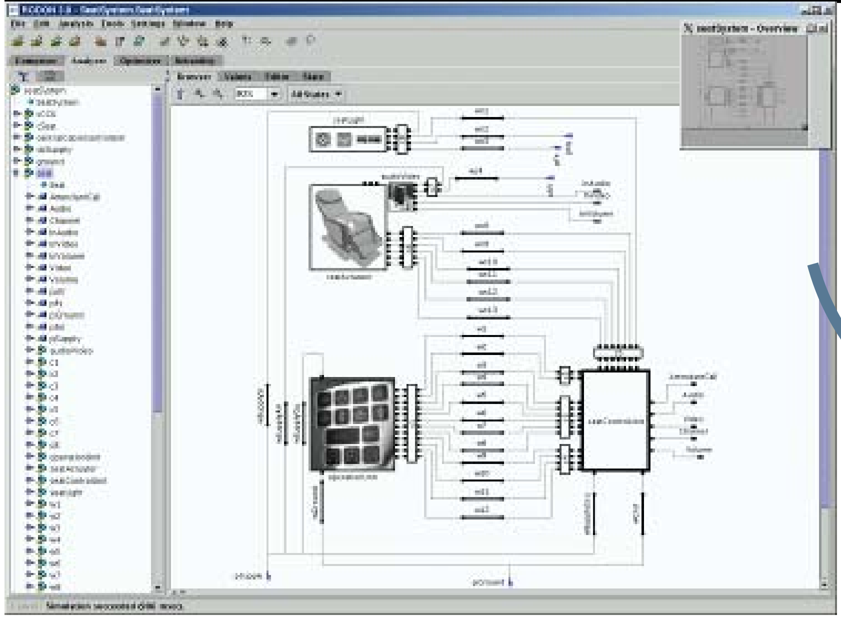
textbook

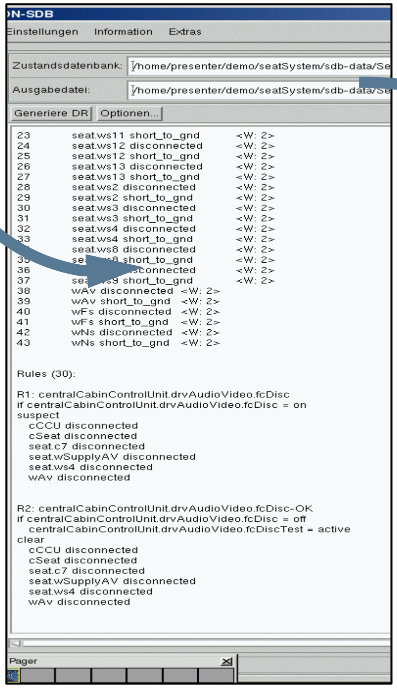
First principle

Predicted behavior

Diagnosis

Diagnostic Rules





```
N-SDB
Einstellungen   Information   Extras

Zustandsdatenbank: /home/presenter/demo/seatSystem/sdb-data/Se
Ausgabedatei:      /home/presenter/demo/seatSystem/sdb-data/Se

Generiere DR   Optionen...

23        seat.ws11 short_to_gnd      <W: 2>
24        seat.ws12 disconnected      <W: 2>
25        seat.ws12 short_to_gnd      <W: 2>
26        seat.ws13 disconnected      <W: 2>
27        seat.ws13 short_to_gnd      <W: 2>
28        seat.ws2 disconnected       <W: 2>
29        seat.ws2 short_to_gnd       <W: 2>
30        seat.ws3 disconnected       <W: 2>
31        seat.ws3 short_to_gnd       <W: 2>
32        seat.ws4 disconnected       <W: 2>
33        seat.ws4 short_to_gnd       <W: 2>
          seat.ws8 disconnected       <W: 2>
35        sea  s8 short_to_gnd        <W: 2>
36             sconnected             <W: 2>
37        sea  s9 short_to_gnd        <W: 2>
38        wAv disconnected  <W: 2>
39        wAv short_to_gnd  <W: 2>
40        wFs disconnected  <W: 2>
41        wFs short_to_gnd  <W: 2>
42        wNs disconnected  <W: 2>
43        wNs short_to_gnd  <W: 2>

Rules (30):

R1: centralCabinControlUnit.drvAudioVideo.fcDisc
if centralCabinControlUnit.drvAudioVideo.fcDisc = on
suspect
   cCCU disconnected
   cSeat disconnected
   seat.c7 disconnected
   seat.wSupplyAV disconnected
   seat.ws4 disconnected
   wAv disconnected


R2: centralCabinControlUnit.drvAudioVideo.fcDisc-OK
if centralCabinControlUnit.drvAudioVideo.fcDisc = off
   centralCabinControlUnit.drvAudioVideo.fcDiscTest = active
clear
   cCCU disconnected
   cSeat disconnected
   seat.c7 disconnected
   seat.wSupplyAV disconnected
   seat.ws4 disconnected
   wAv disconnected

Pager
```

- Generated by systematic computation
- Contains virtually all
- Root cause <=> symptom relationships
- Applicable in Real Time systems
- Finds single & multiple faults
- Interfaces exist to various embedded systems exist

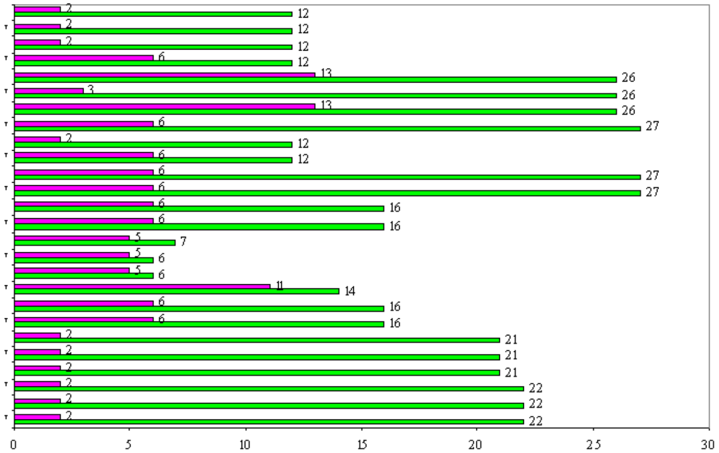
Resources Diagnostic Engine:

- 16 Bit µ-processor, 25 Mhz
- 118 KB Flash memory

Resources Diagnostic Application:

- Compiled model < 2KB
- Some 20 msec time

Diagnostics Rules

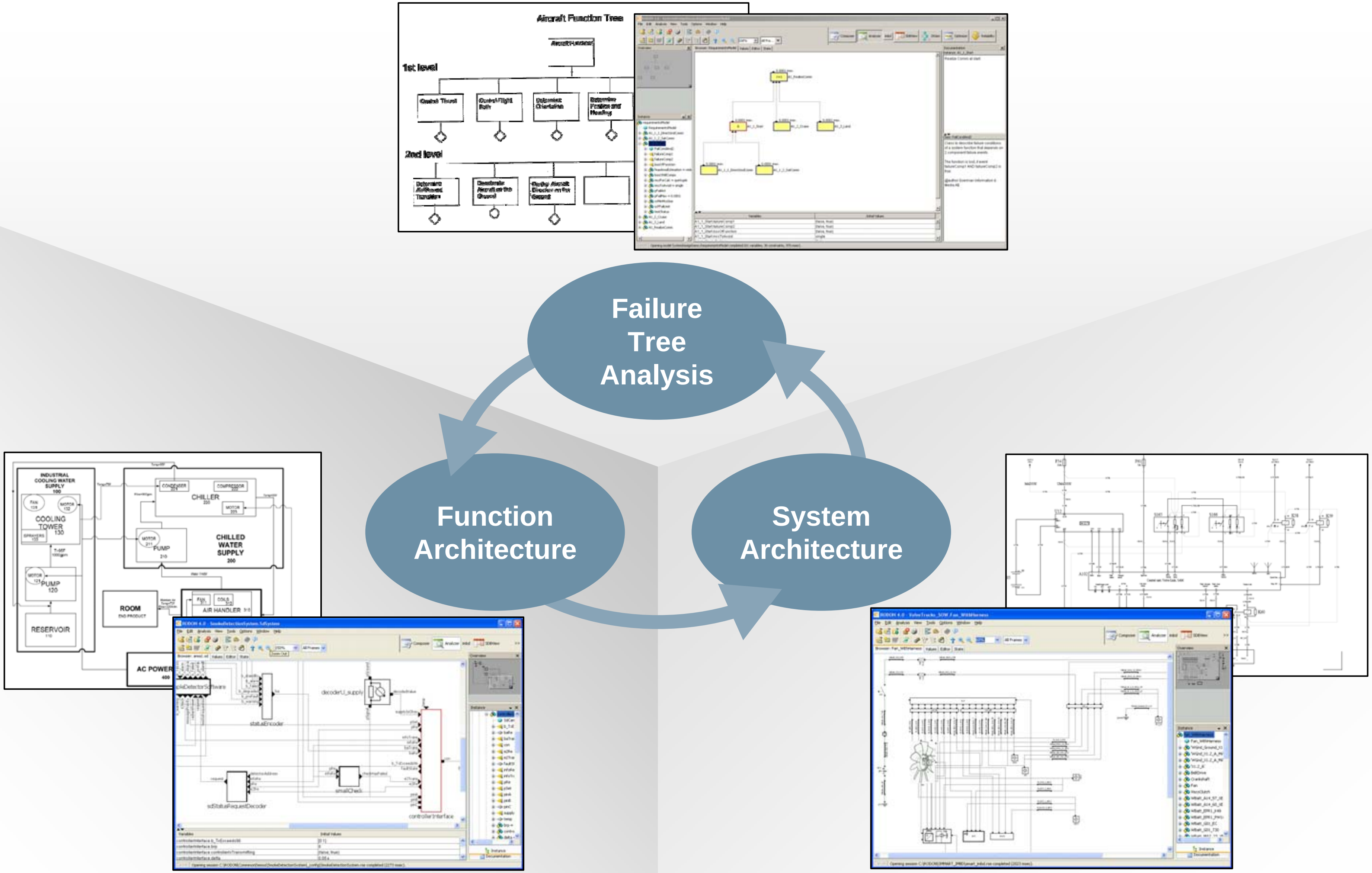


- Diagnostic Rules (SD) applied On Board the Mercedes-Benz SL-Class
- Monitors some 1500 EE parts (Body)
- Reduced effort in service bay

- Usually based on self diagnosis (BITE)
- Reduces # of candidates greatly
  - Green bars: # of candidates per DTC system (BITE)
  - Purple bars: # of candidates per System Diagnosis (SD)
- Identifies true candidates

- RODON Real Time DR Engine tested successfully in a test bench environment
- Met all resource & diagnostic requirements

The different views/stages in System Design



Failure Tree Analysis

Function Architecture

System Architecture

Conclusions

- Today's challenges and trends:
  - Complexity
  - Variants
  - Info drop
- End-to-end solution from Design to Service Stations
- Model Based Design
  - Ranges from Manual authoring to Complete Model Based
  - Easy entry
  - Still Extendable
  - Future proof
  - Always with full integration of information