UPTIME®

Towards a Model-Based Safety Assessment Process of Safety Critical Embedded Systems

Peter Bunus
petbu@ida.liu.se

Personal Presentation

Peter Bunus

Product and Technology Manager

Responsible with the Technical Development of RODON, a model-based diagnostics system used by avionics and automotive industry

peter.bunus@uptimeworld.com

Part Time (15%) Assistant Professor at the Department of Computer and Information Science, Linköping University, SWEDEN

- Course Leader and Examiner for TDDB84 Design Patterns
- Research on modeling and simulation languages, model-based software development, program static analysis and verification, debugging, diagnosis
- Programming environments

How to Prevent Failures

- Todays lecture will be about how to prevent failures
  - What is needed to be done during the design process
  - What can be done after the system is deployed to minimize failure effects

Picture taken by Janis Krums


Picture from Radio Nederland Wereldomroep

Picture from Radio Nederland Wereldomroep

Attributes of Dependability

- IFIP WG 10.4 definitions
  - Safety: absence of harm to people and environment
  - Availability: the readiness for correct service
  - Integrity: absence of improper system alterations
  - Reliability: continuity of correct service
  - Maintainability: ability to undergo modifications and repairs

Maintainability

Models of After Sales Services

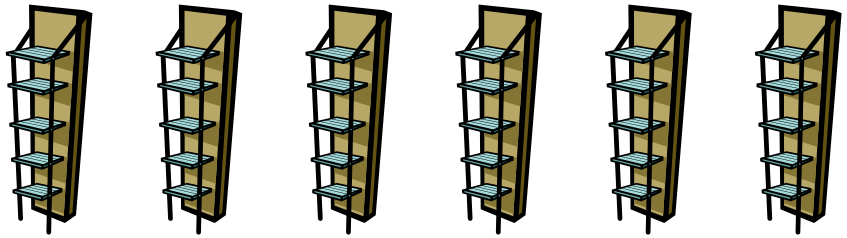
Service priority	Business model	Terms	Example	Product owner
None	Disposal	Dispose of products when they fail or need to be upgraded	Razor blades	Consumer
Low	Ad hoc	Pay for support as needed	TVs	Consumer
Medium-high	Warranty	Pay fixed price as needed	PCs	Consumer
Medium-high	Lease	Pay fixed price for a fixed time; option to buy product	Vehicles	Manufacturer;
High	Cost-plus	Pay fixed price based on cost and pre-negotiated margin	Construction	leasing company
Very high	Performance based	Pay based on product's performance	Aircraft	Customer
Very high	Power by the hour	Pay for services used	Aircraft engines	Customer

Geographical Hierarchy

Central repair facility, spare parts warehouse, and distribution center

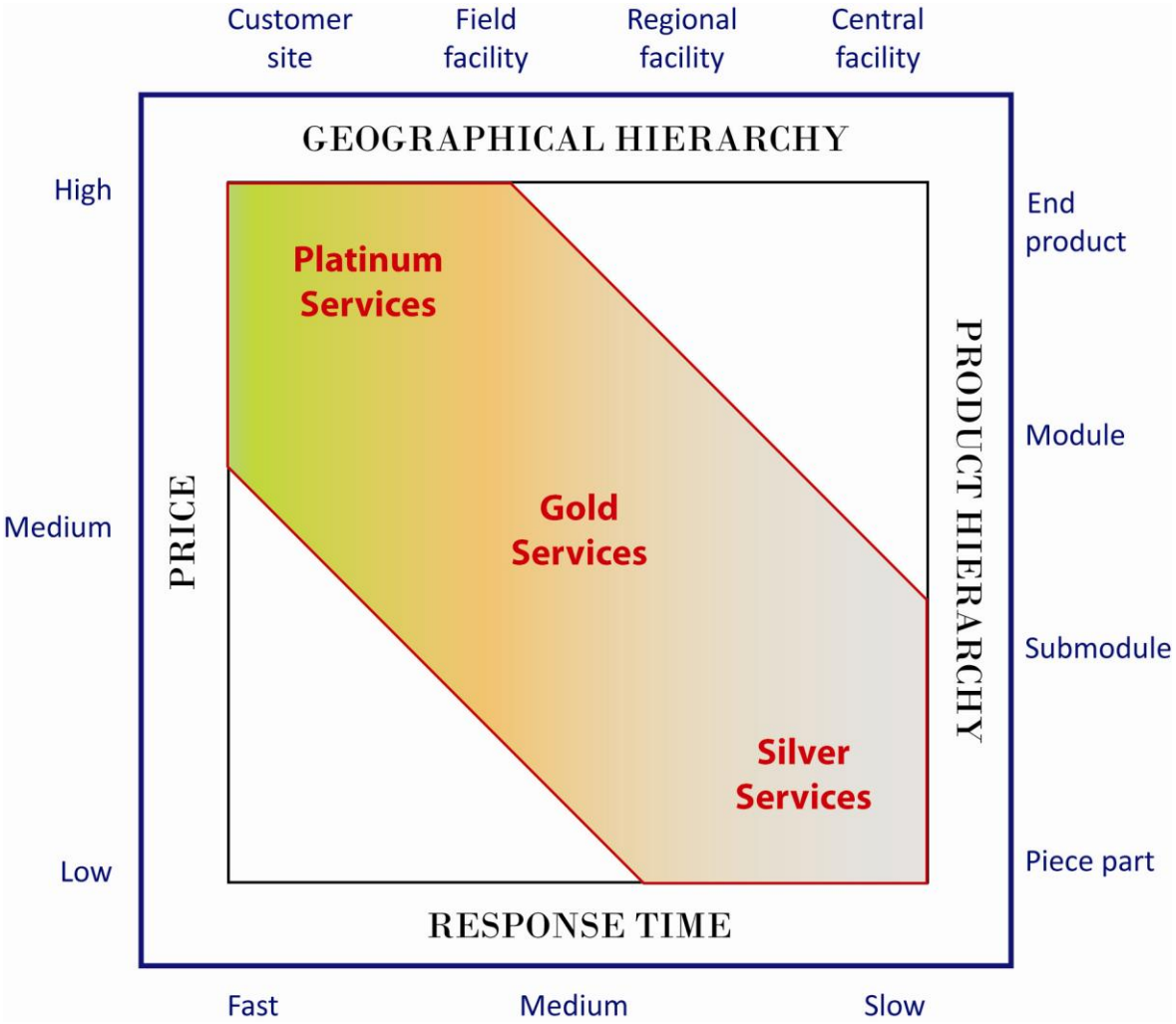
Regional repair facilities and spare parts distribution centers

Field repair facilities and spare parts distribution centers



Stocks of spare parts on-site with customers

After Sales Services



Houston – We've had a problem

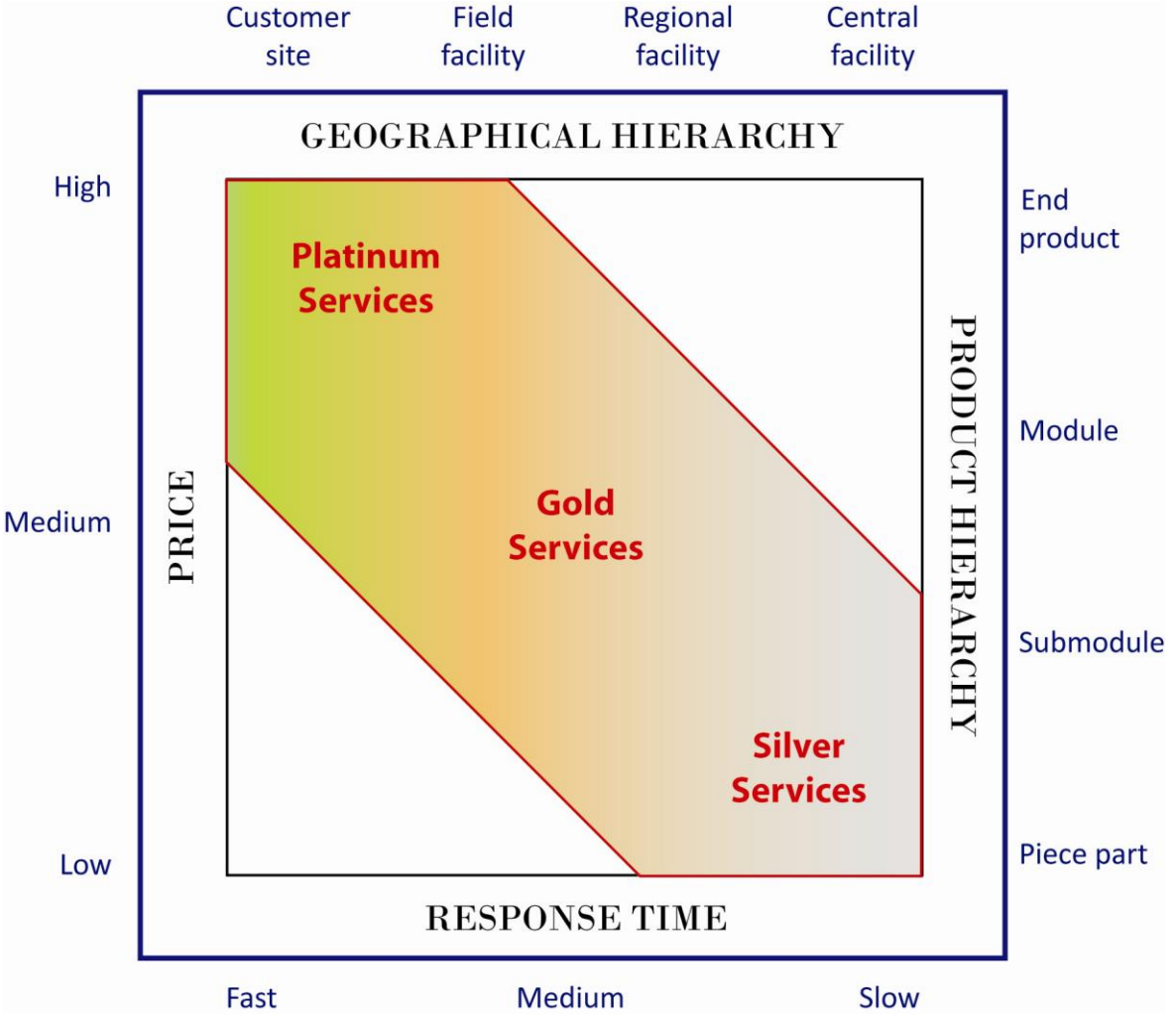
02 07 55 19	LMP	Okay, Houston - -
02 07 55 20	CDR	I believe we've had a problem here.
02 07 55 28	CC	This is Houston. Say again, please.
02 07 55 35	CDR	Houston, we've had a problem. We've had a MAIN B BUS UNDERVOLT.
02 07 55 42	CC	Roger. MAIN B UNDERVOLT.
02 07 55 58	CC	Okay, stand by, 13. We're looking 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.

Houston – We've had 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.

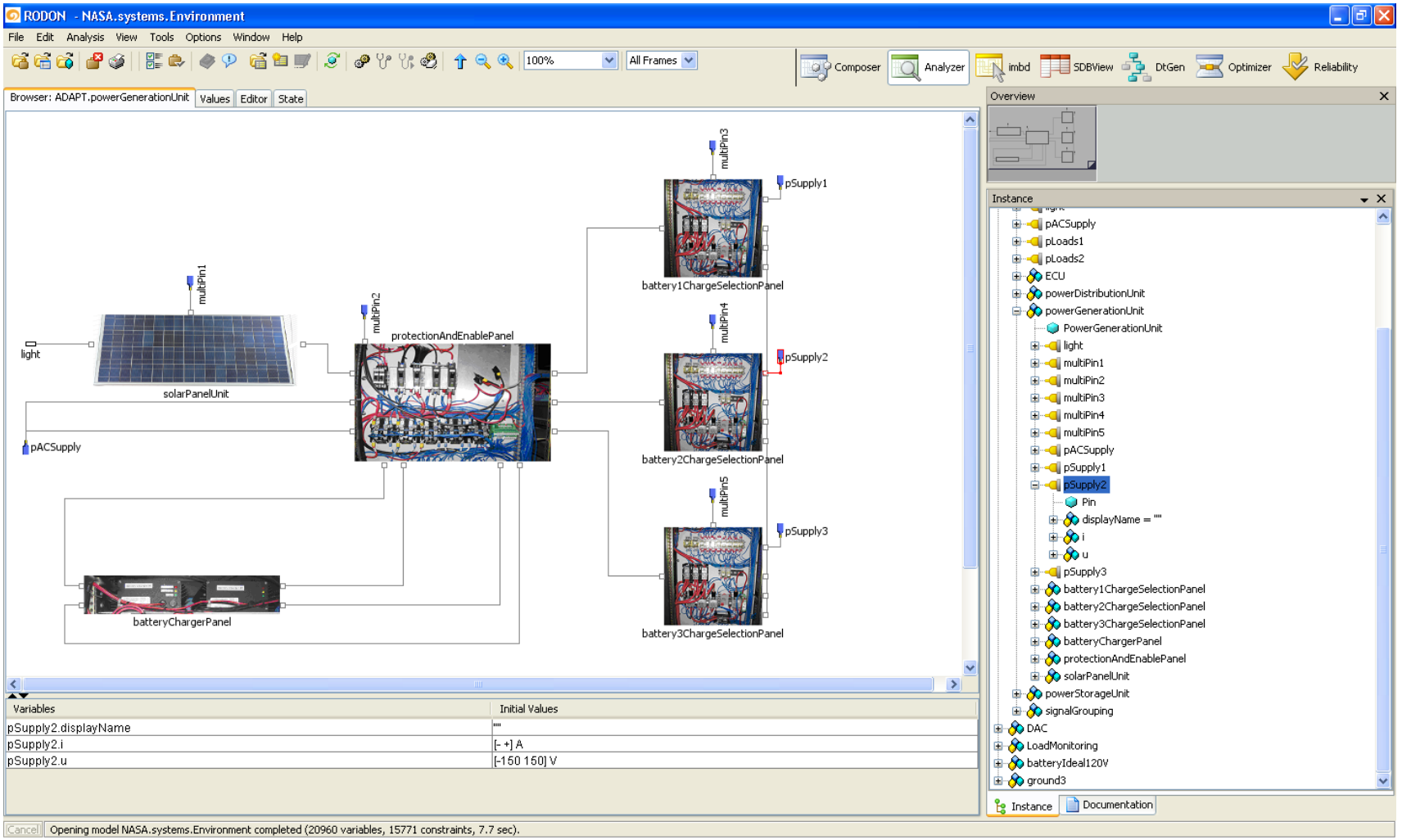
What do you think?

- Which kind of Services do we need to provide to the Apollo 13 crew members?



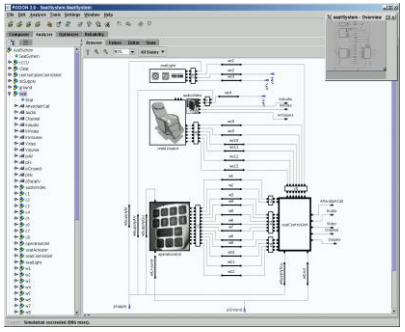
“Well HAL, I’m damned if I can find anything wrong with it.”
“Yes. It’s puzzling. I don’t think I’ve ever seen anything quite like this before.”
-- *2001: A Space Odyssey*

Model of the NASA ADAPT Satellite System



Model-Based Diagnosis Principles

Actual system
Passenger seat system



Model of the passenger seat system

Corrections repair actions

Observations

Observed behavior

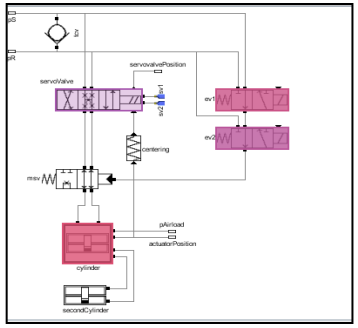
Diagnosis

Diagnostic Reasoner

Predicted behavior

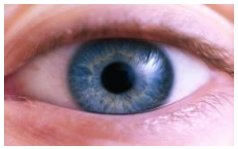
Simulation

The Diagnostic Problem



Design
Structural
Description

*V=i*R*
Domain Knowledge
Component



Measurements/
Observations

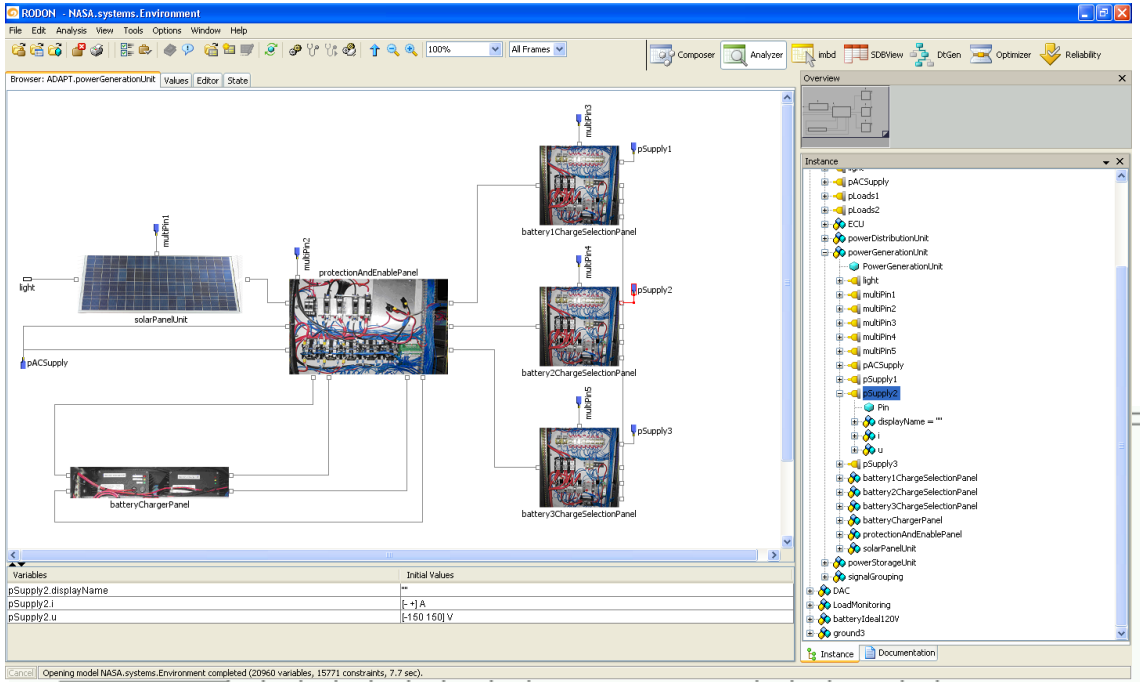
X=6V

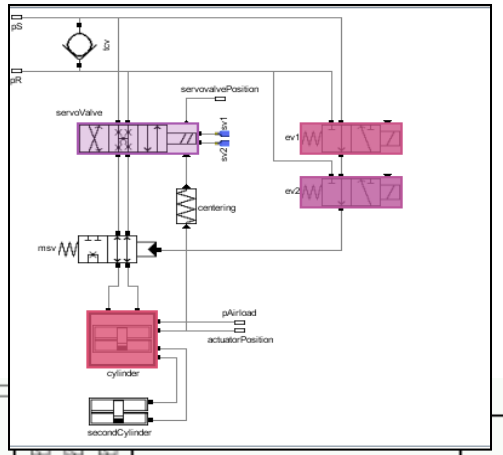
Diagnostic
Reasoner

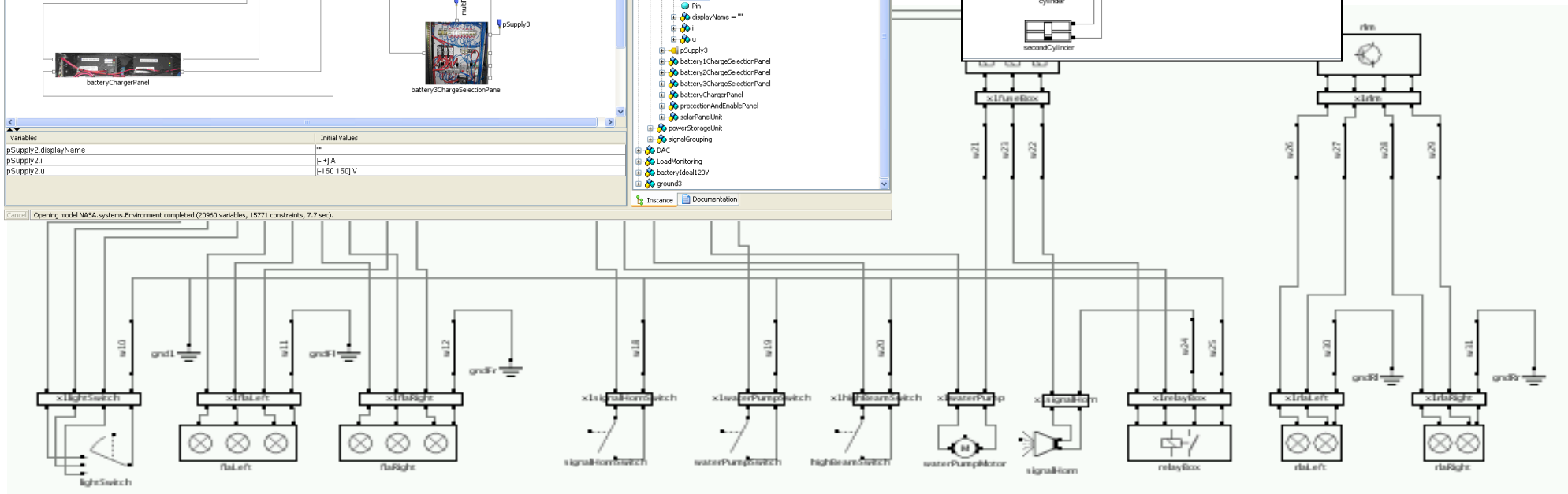
Diagnosis
Repair Actions

Replace servoValve

Where the Model Comes From?

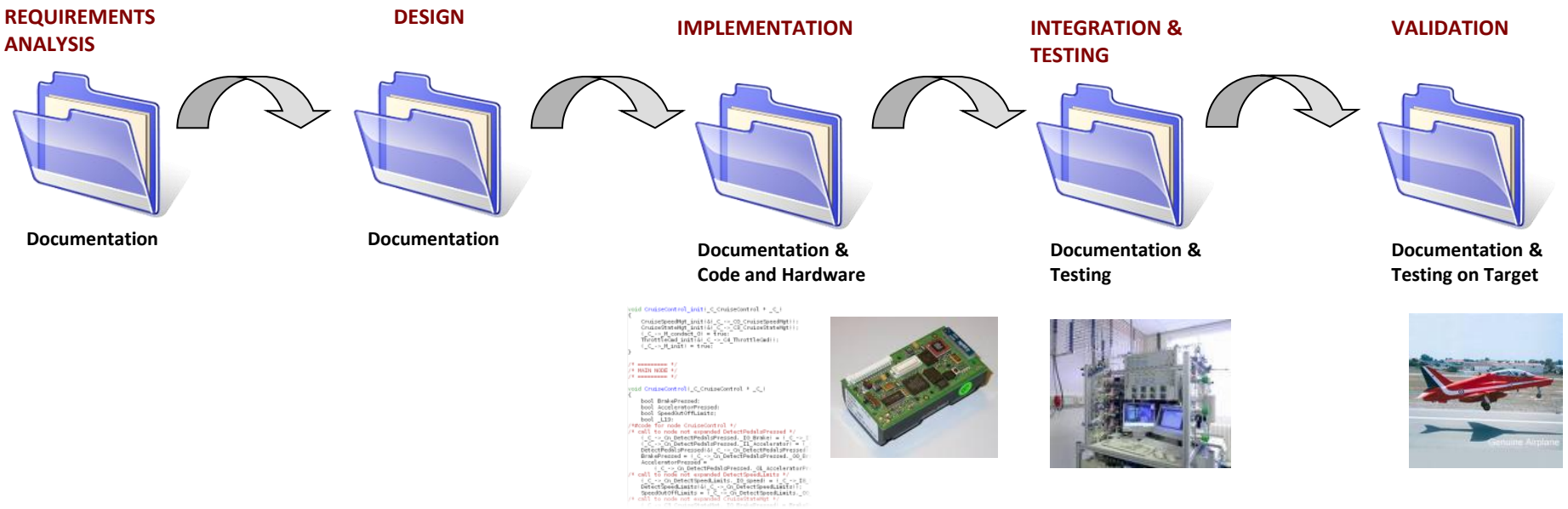




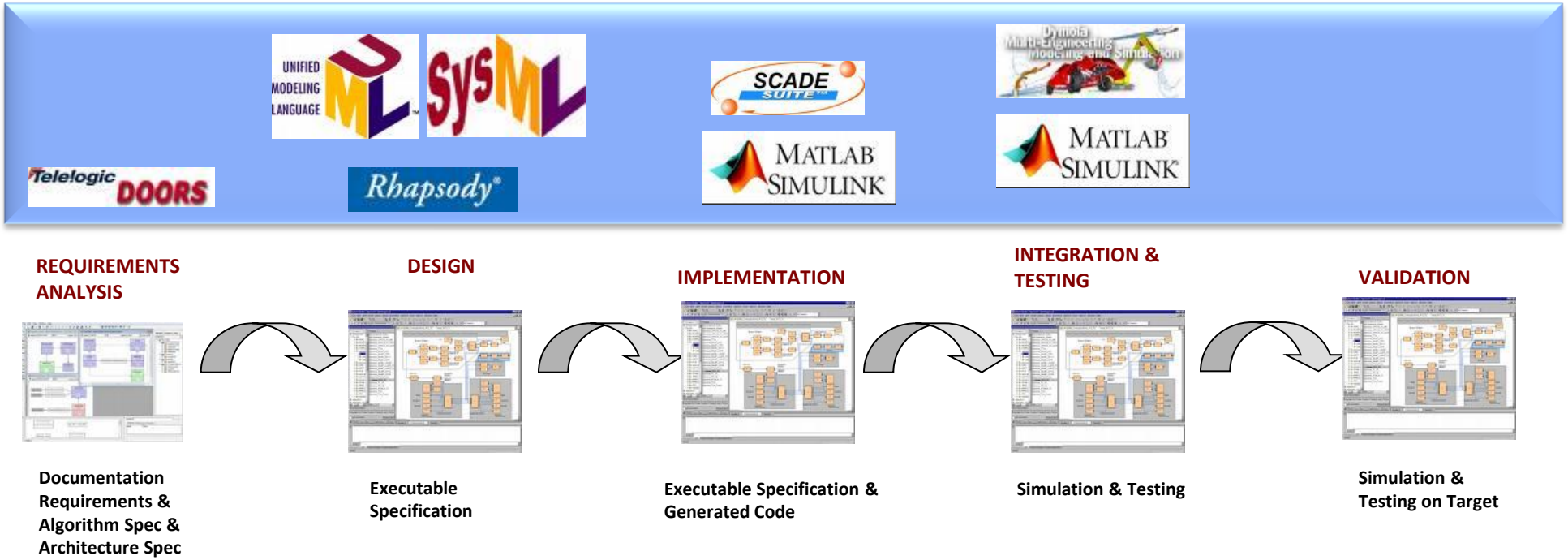


Traditional Design Flow

- 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

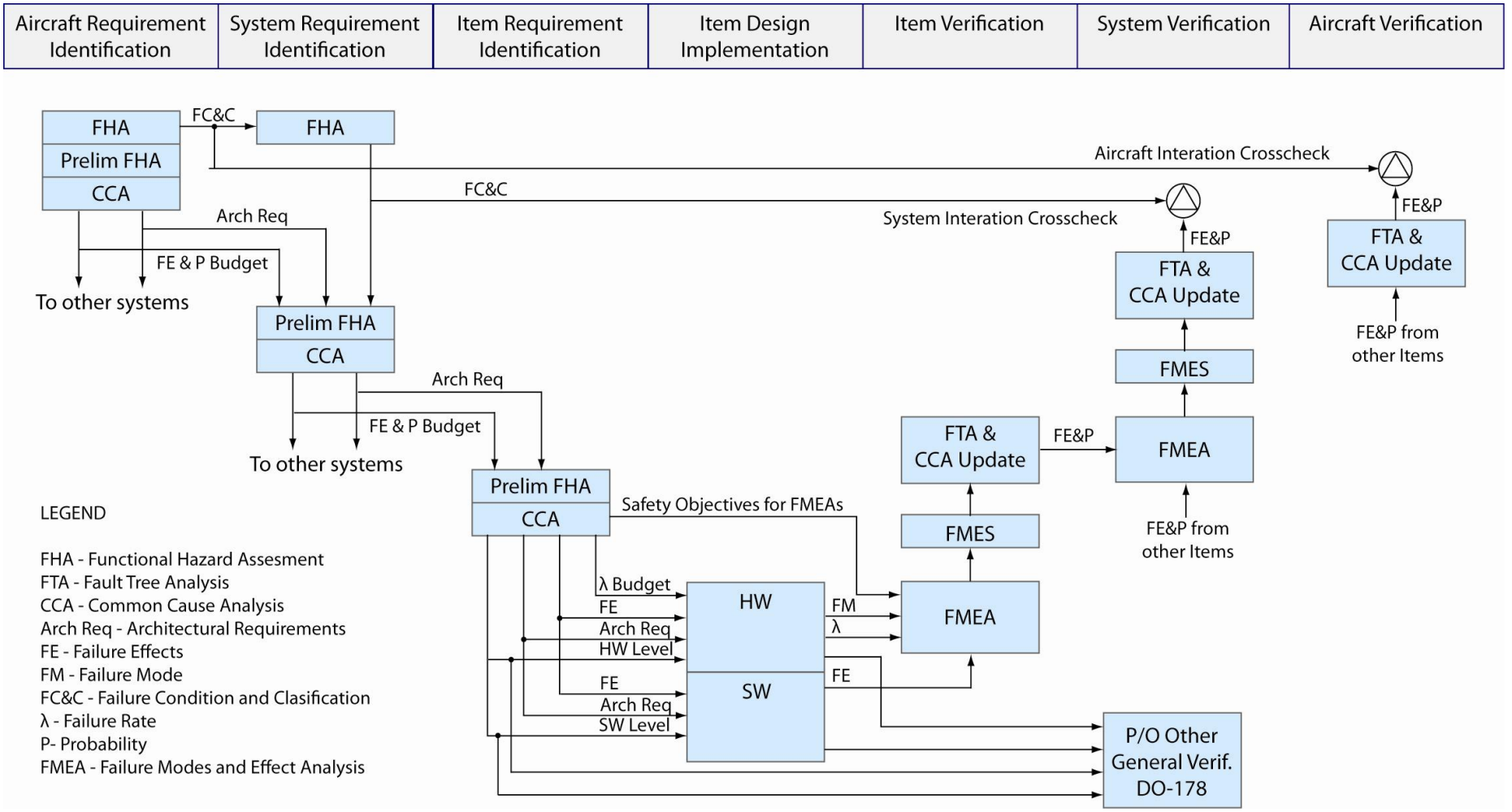


Model-Based Design



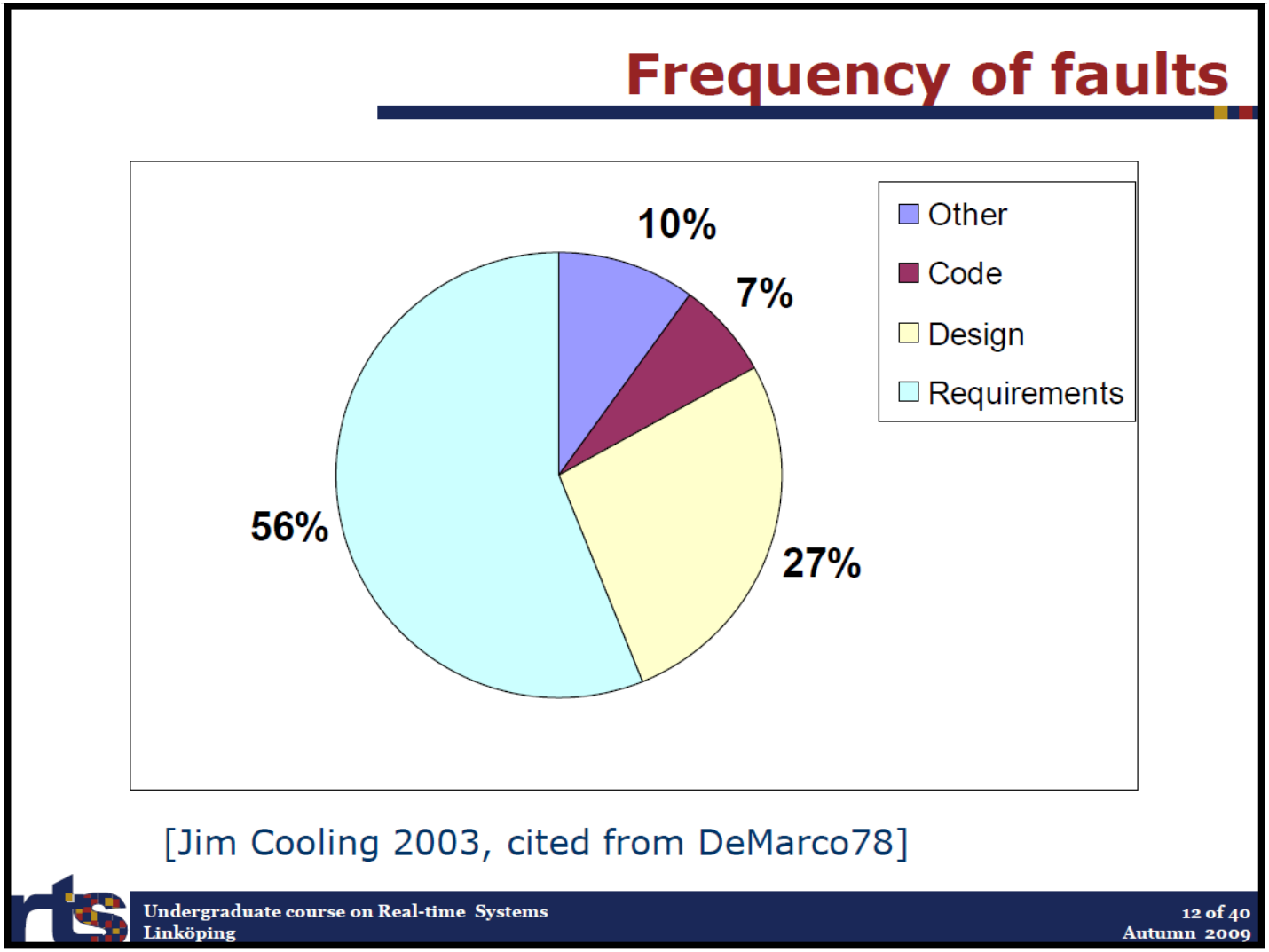
- Model-Based Design Flow
  - Build explicit architectures of predictable systems
  - Go seamlessly from abstraction to realizations
  - Capitalize on verification activities early and all along the development flow

ARP 4754 Safety Assessment Diagram



SAE ARP 4754 "Certification Considerations for Highly-Integrated or Complex Aircraft Systems

Frequency of Faults



Traditional Model Development

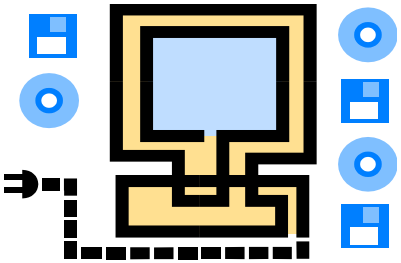
Technology expert

Technology expertise

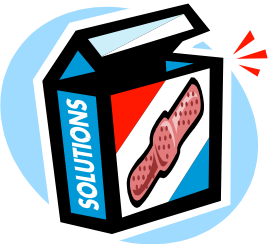
Platform expert

Platform expertise

Domain analysts, Modelers, Designers, Developers



Traditional Development Tools



Application

Domain experts

Domain expertise

UPTIME®

MDA-Based Modeling and Development

Technology expert

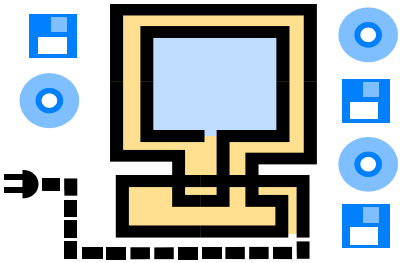
Technology expertise

Application Developers

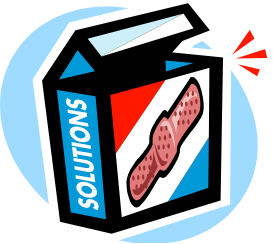
Implementation expertise

Platform expert

Platform expertise



MDA Tools

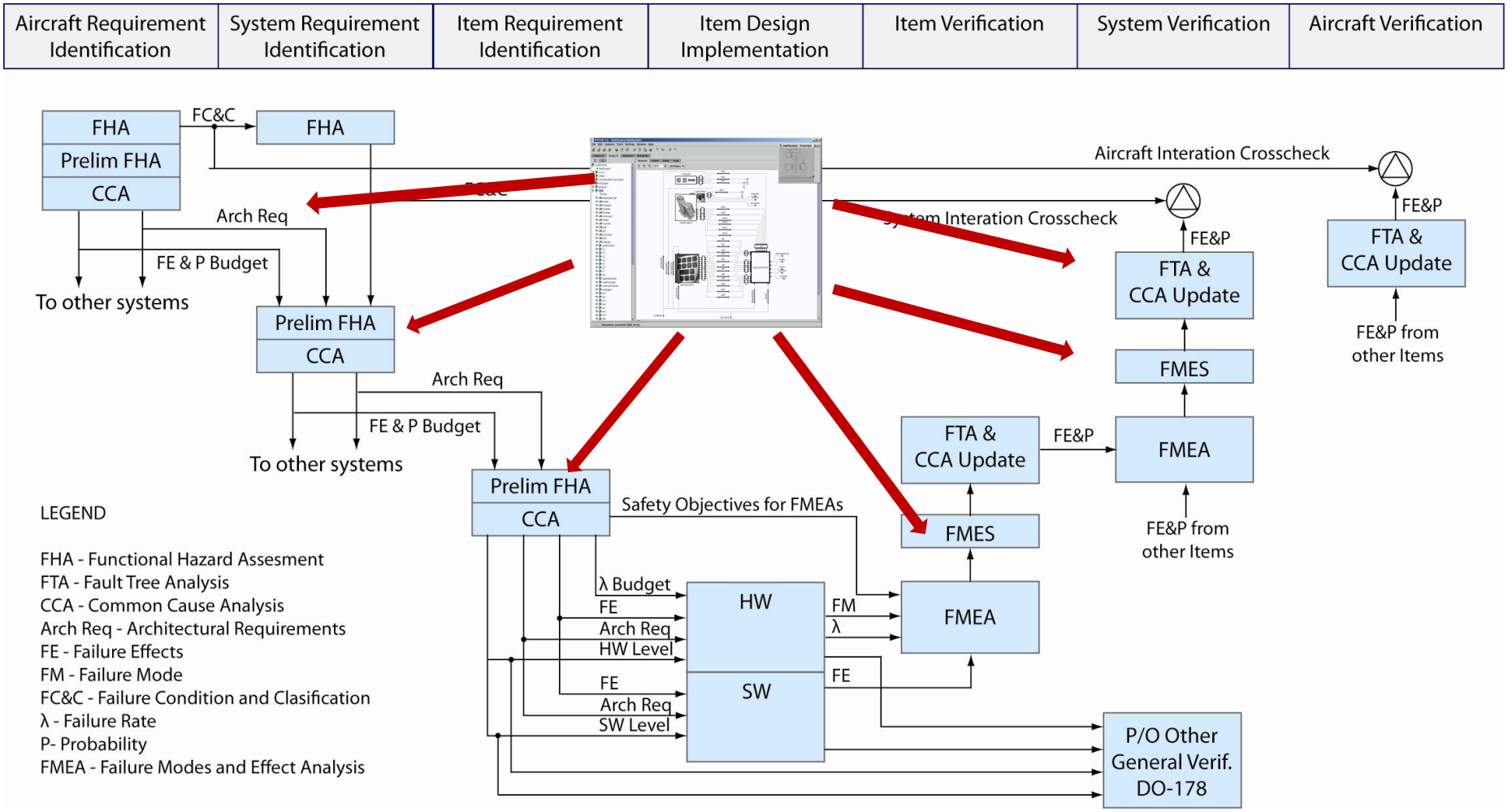


Application

Domain expertise

Domain experts

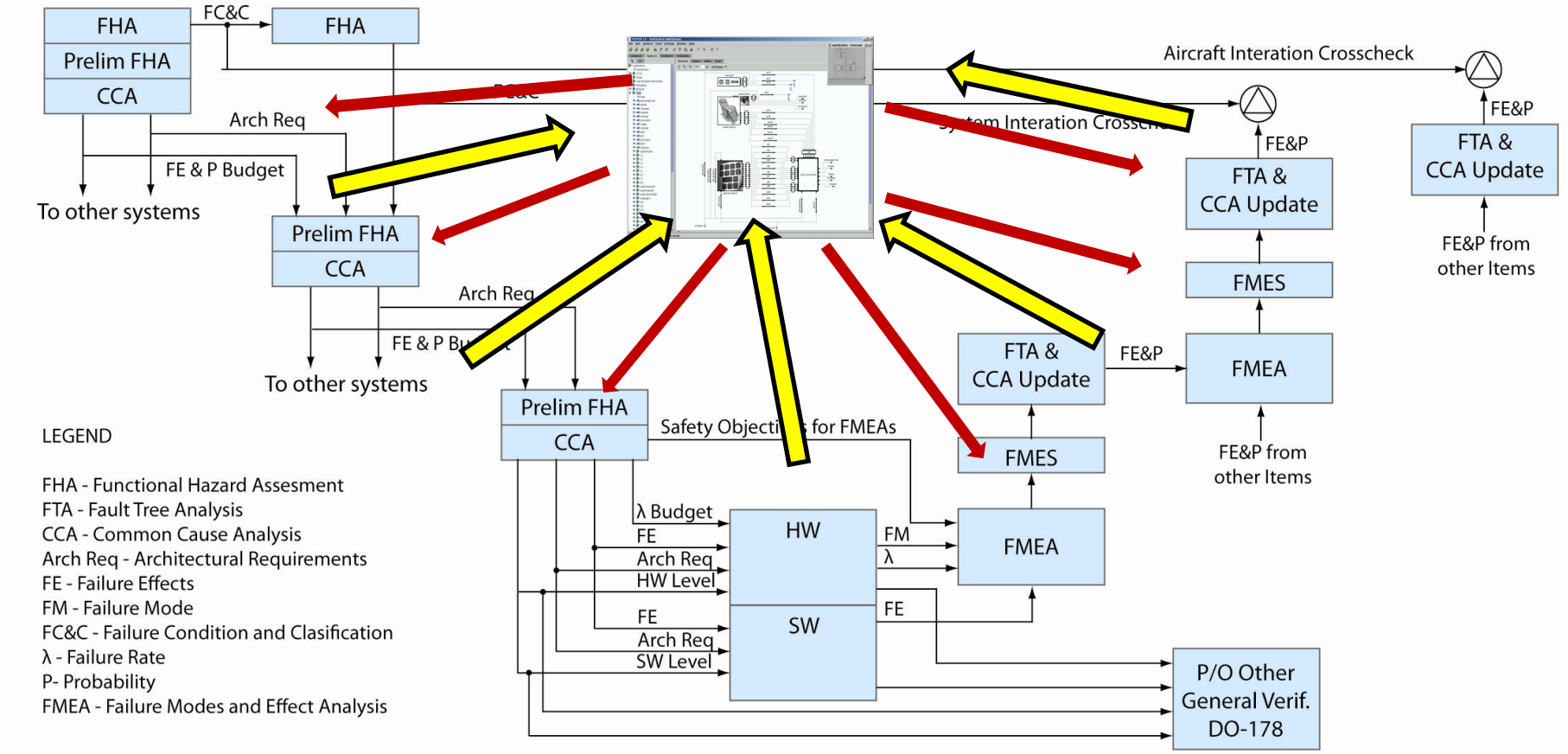
Model-Based Approach to Safety Assessment



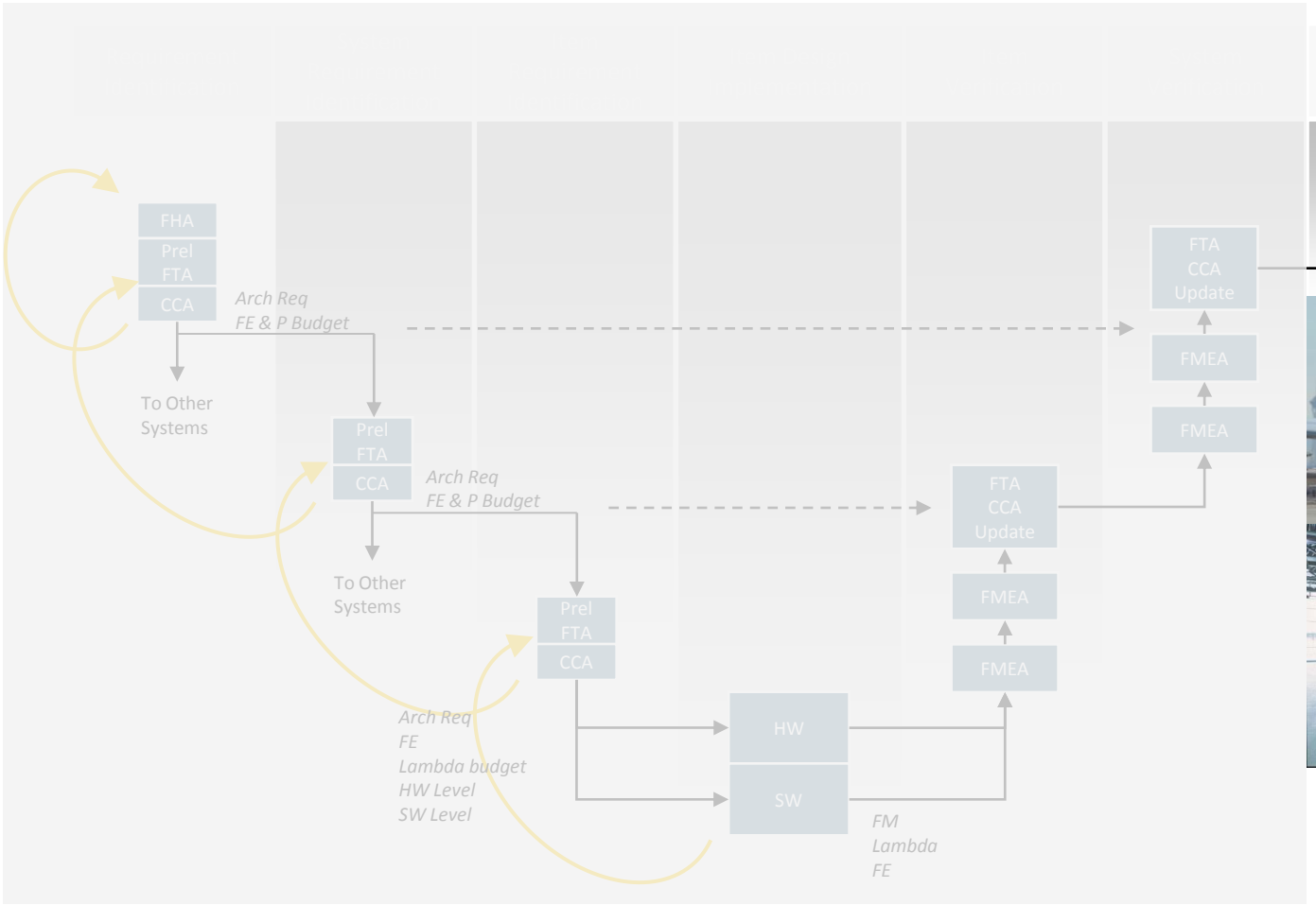
SAE ARP 4754 "Certification Considerations for Highly-Integrated or Complex Aircraft Systems

Flexibility in Supporting the Process

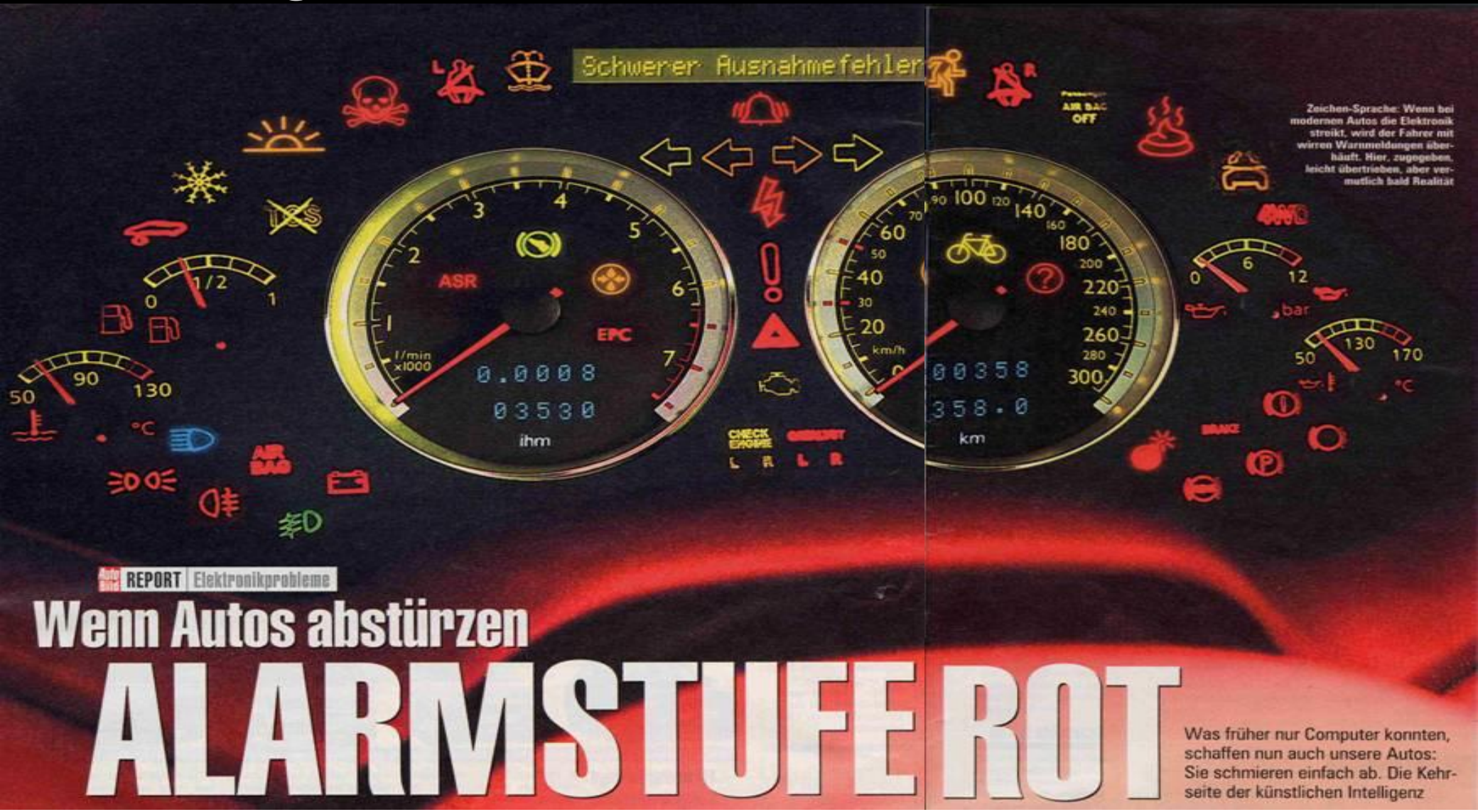
Aircraft Requirement Identification	System Requirement Identification	Item Requirement Identification	Item Design Implementation	Item Verification	System Verification	Aircraft Verification



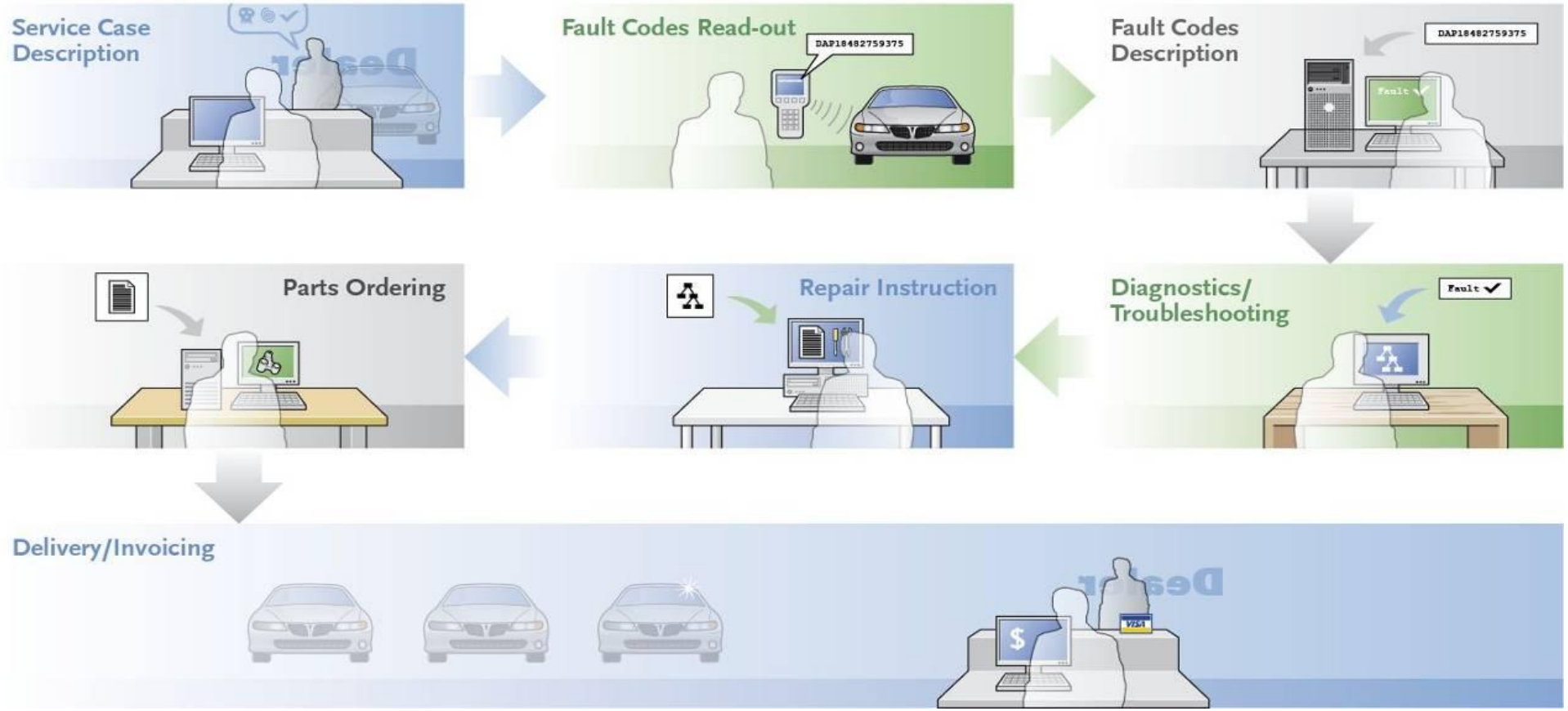
Vehicle Verification Stage



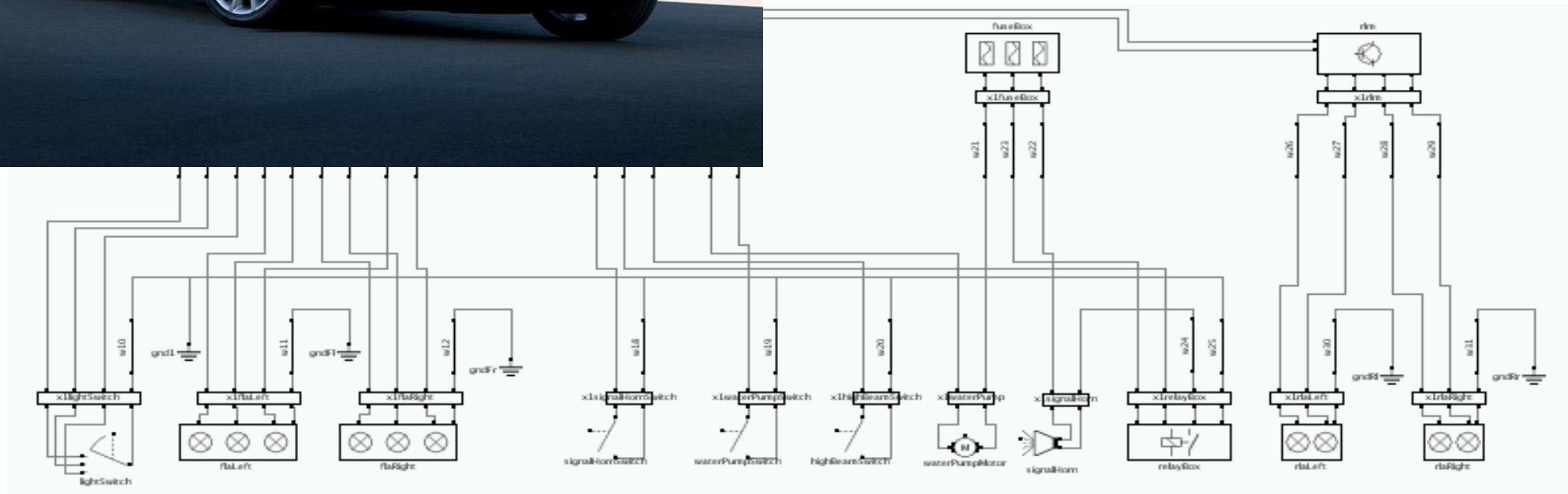
The Diagnosis Problem



Traditional Service Process



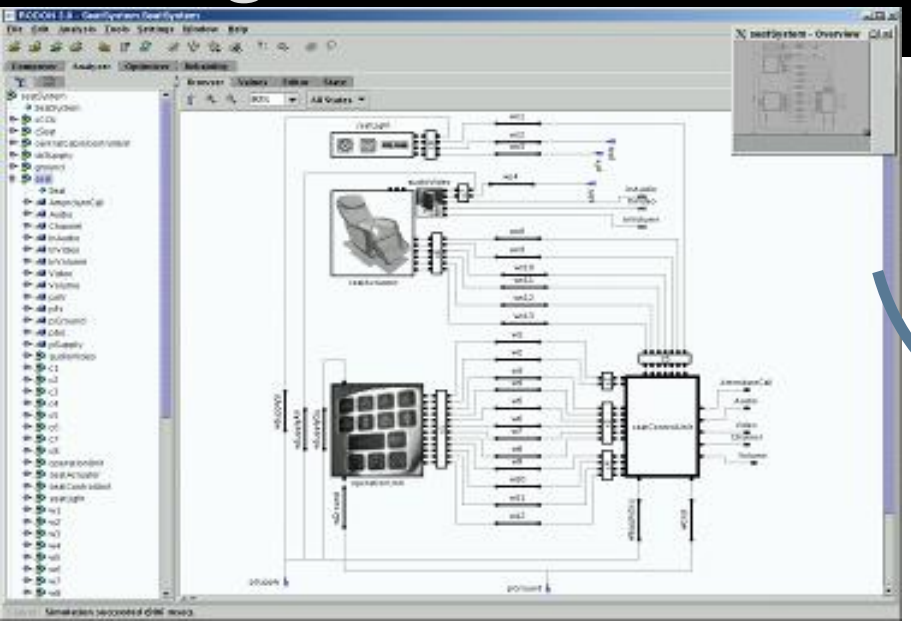
Tutorial Demo Exterior Lighting

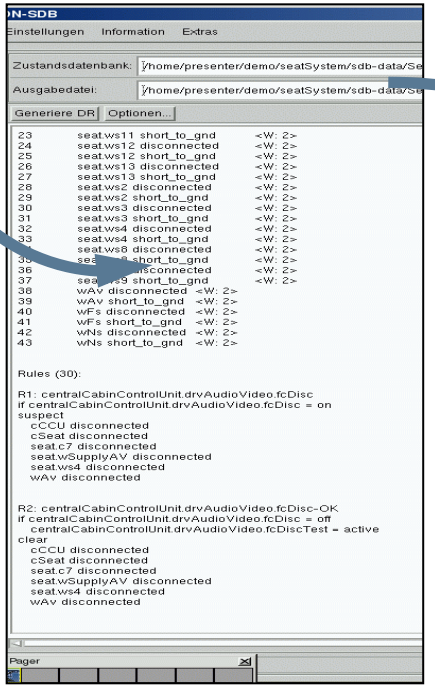



...IS VÖLLIG NORMAL, ERWIN! HEUTZUTAGE SIND ALLE MODERNEN FAHRZEUGE MIT ELEKTRONIK VOLLGESTOPFT!
R-ELEKTRONIK

Model-Based Diagnostics in Practice

Diagnostic Rules





- 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

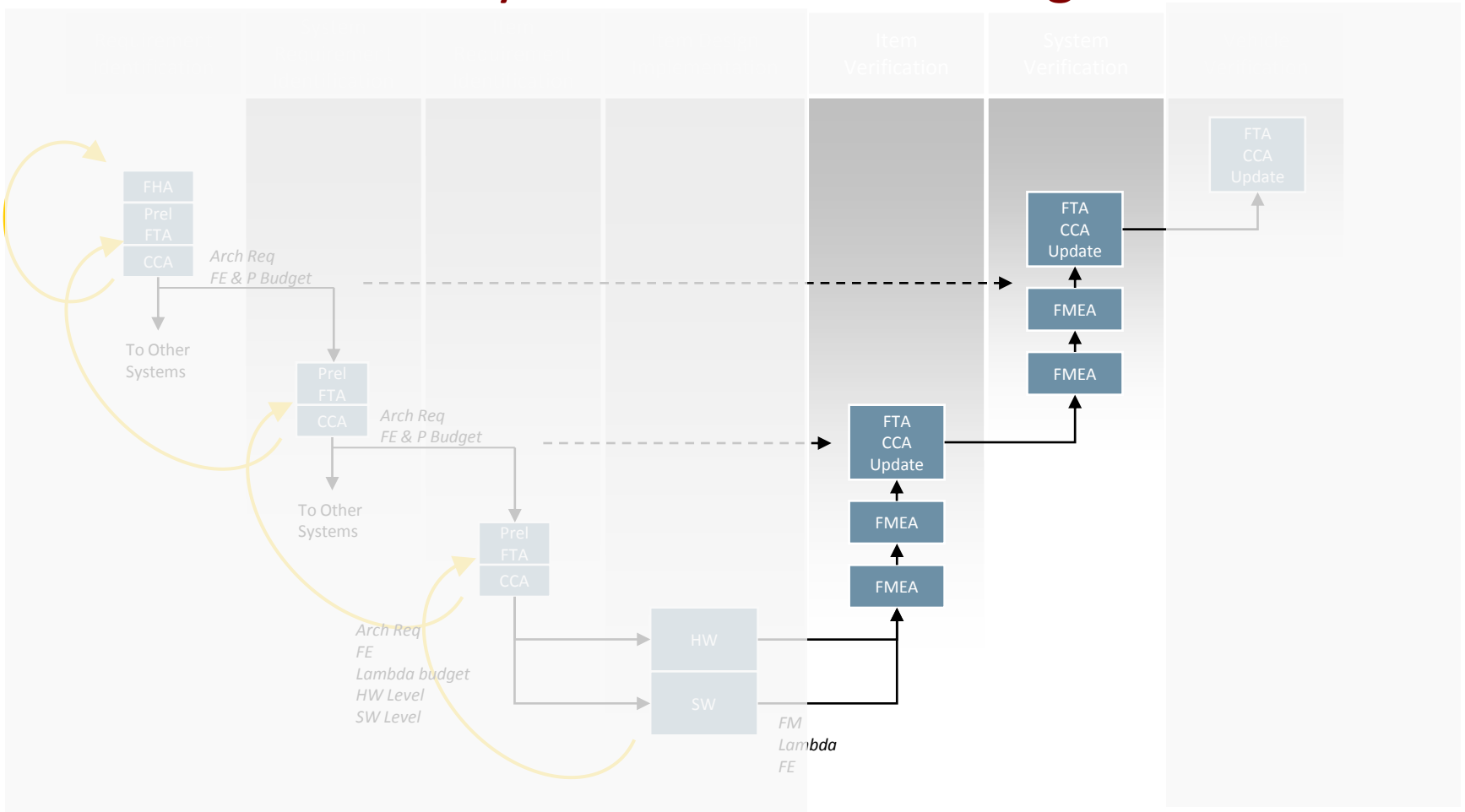
Resources Diagnostic Engine:

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

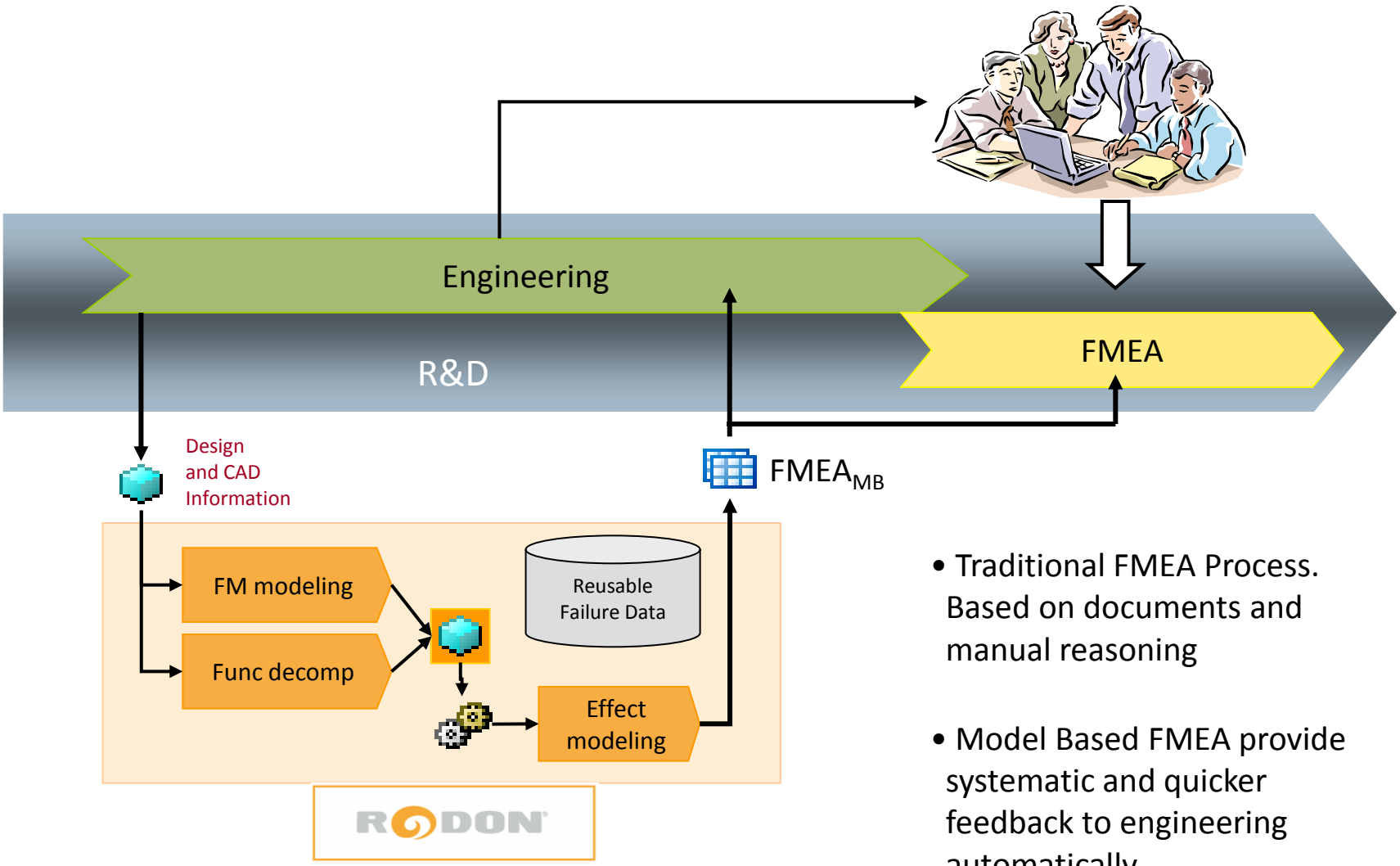
Resources Diagnostic Application:

- Compiled model < 2KB
- Some 20 msec time

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

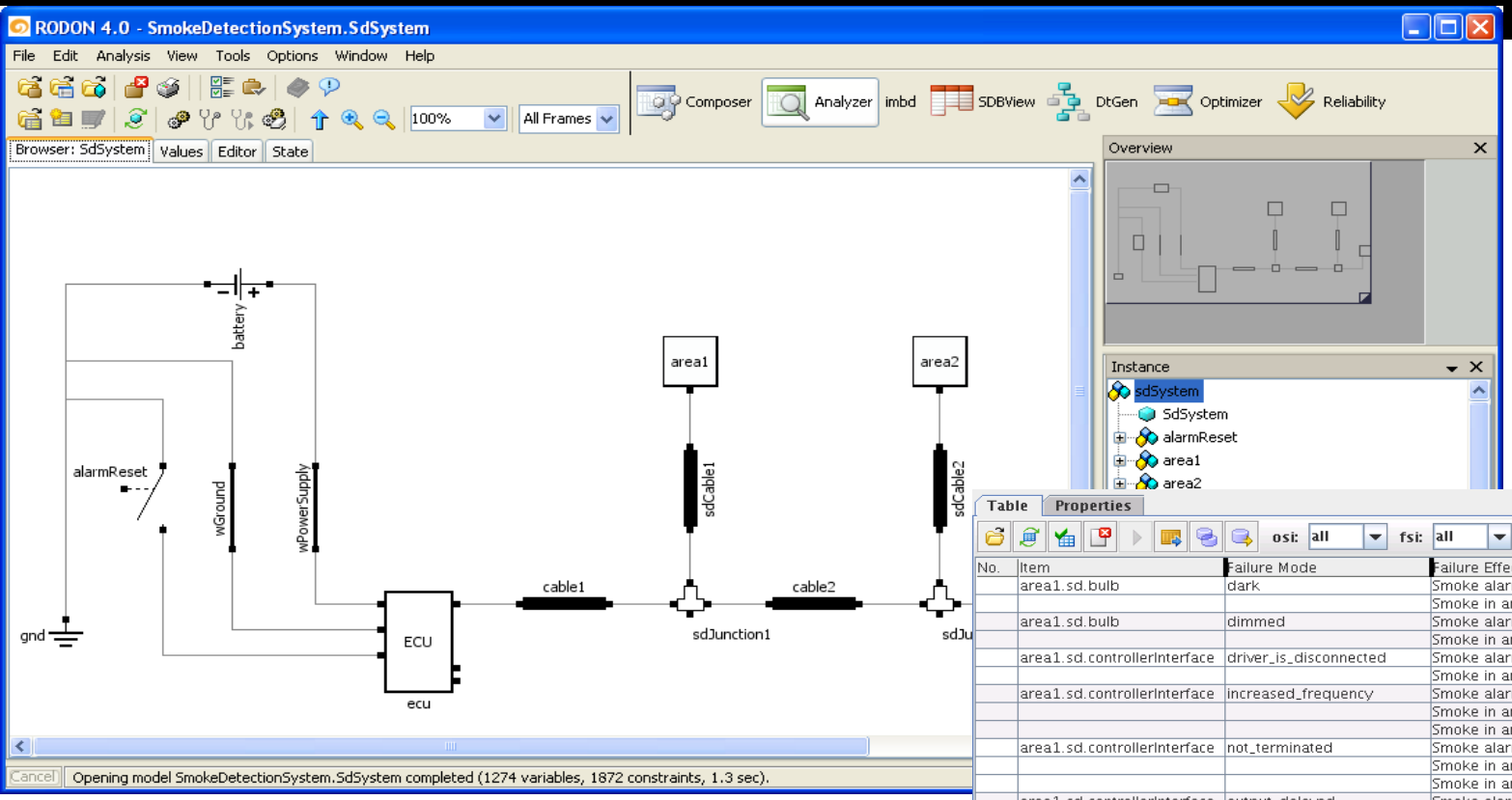
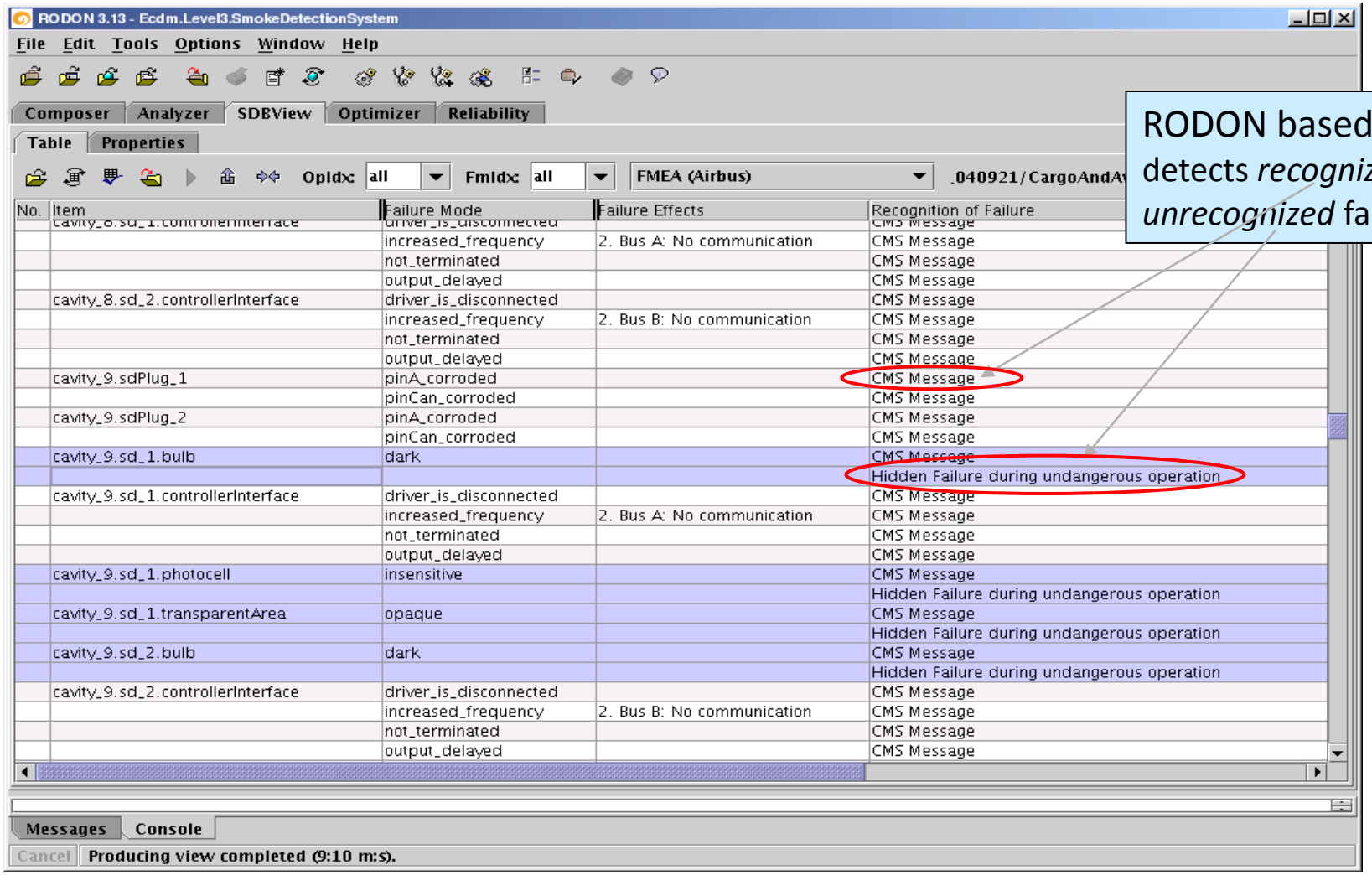


Table | Properties

osi: all fsi: all FMEA (SDS) sdb-data/sm

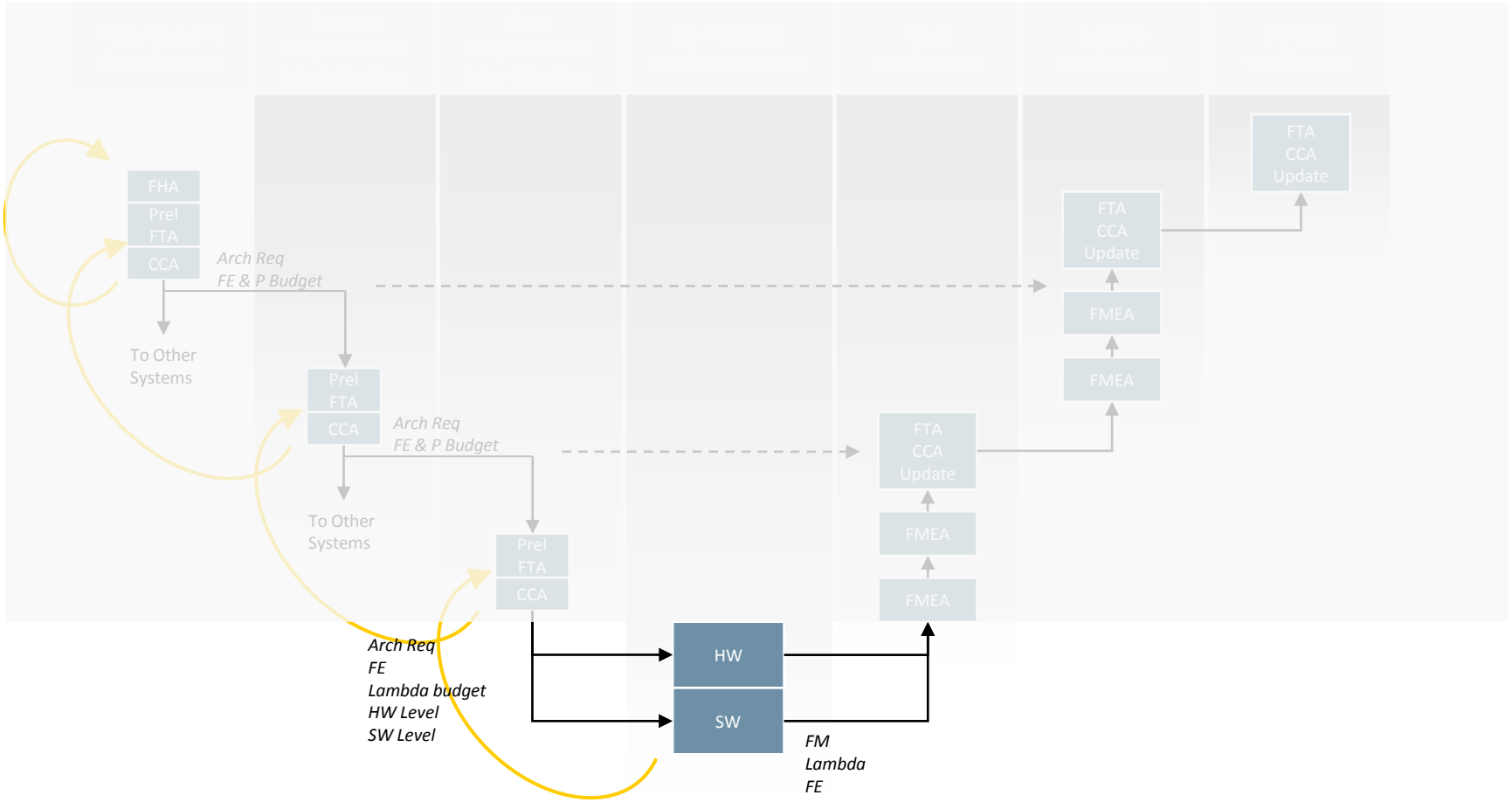
No.	Item	Failure Mode	Failure Effects	Recognition of Failure
	area1.sd.bulb	dark	Smoke alarm is different from ok-case	Failure indication during test
			Smoke in area1 but no alarm	Hidden failure during operation
	area1.sd.bulb	dimmed	Smoke alarm is different from ok-case	Hidden failure during operation
			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	

Failure Impact on Functions (detected and undetected)

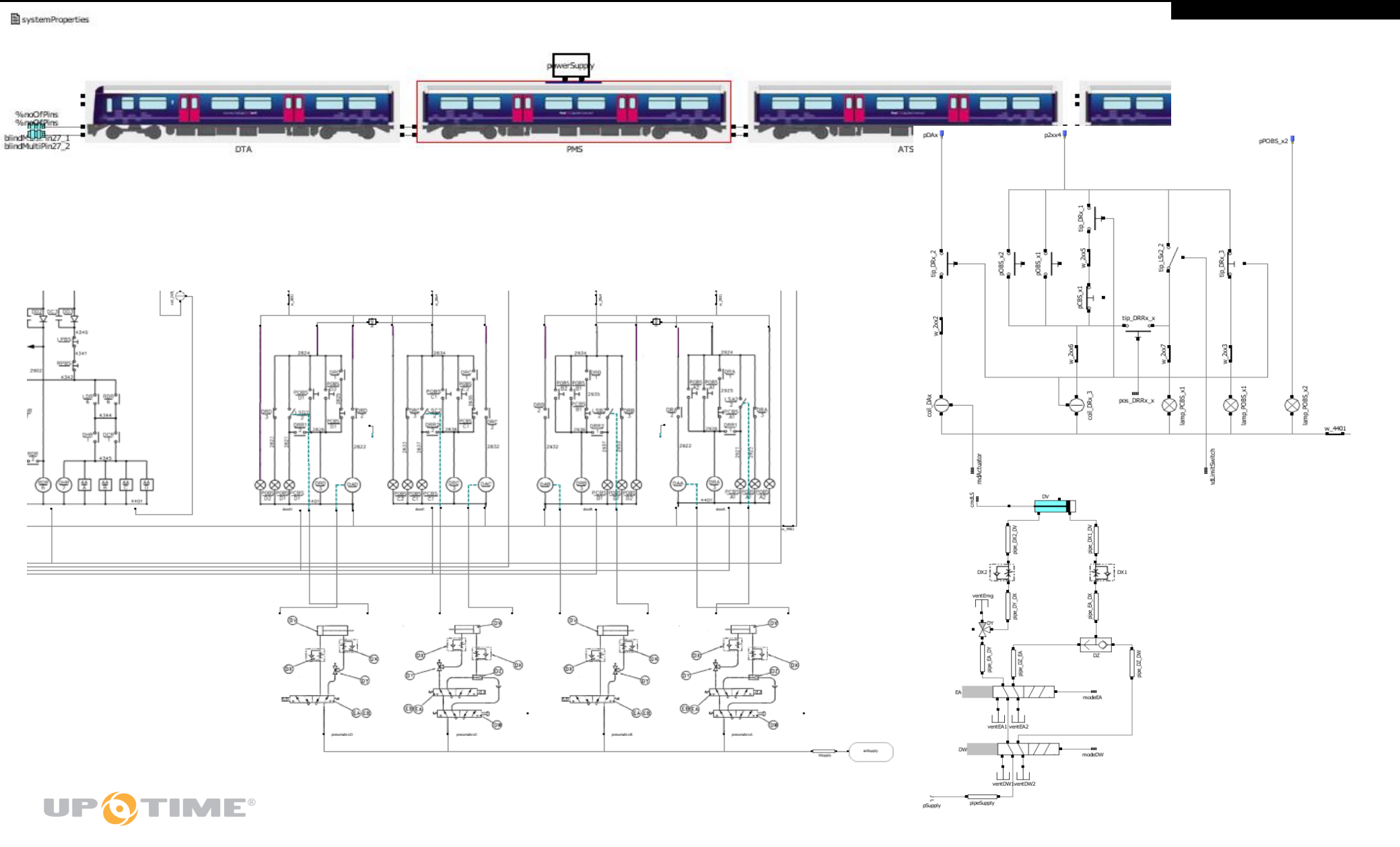


RODON based FMEA detects *recognized* and *unrecognized* failures

Item Design Implementation Stage

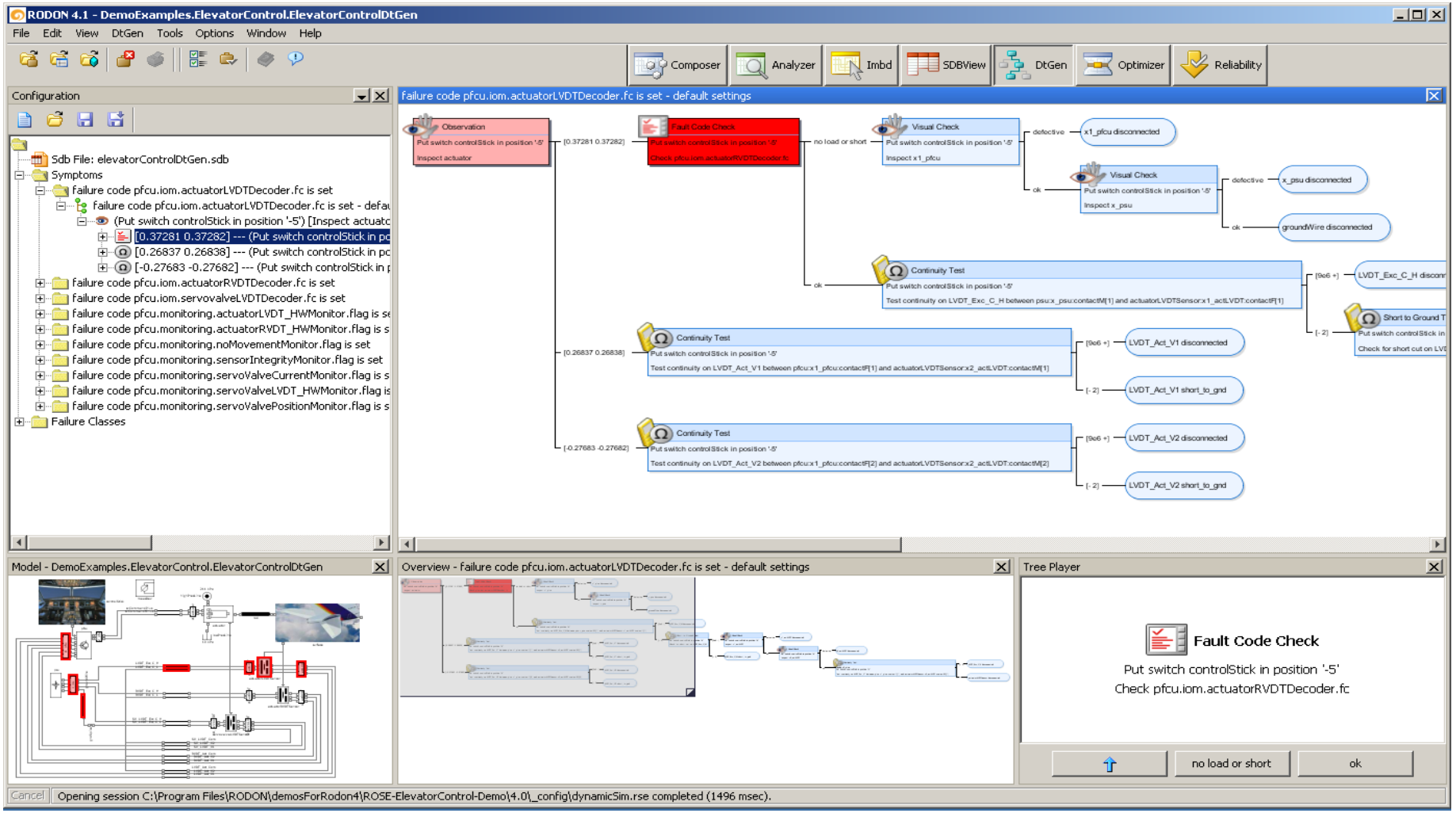


Train Electrical Door System

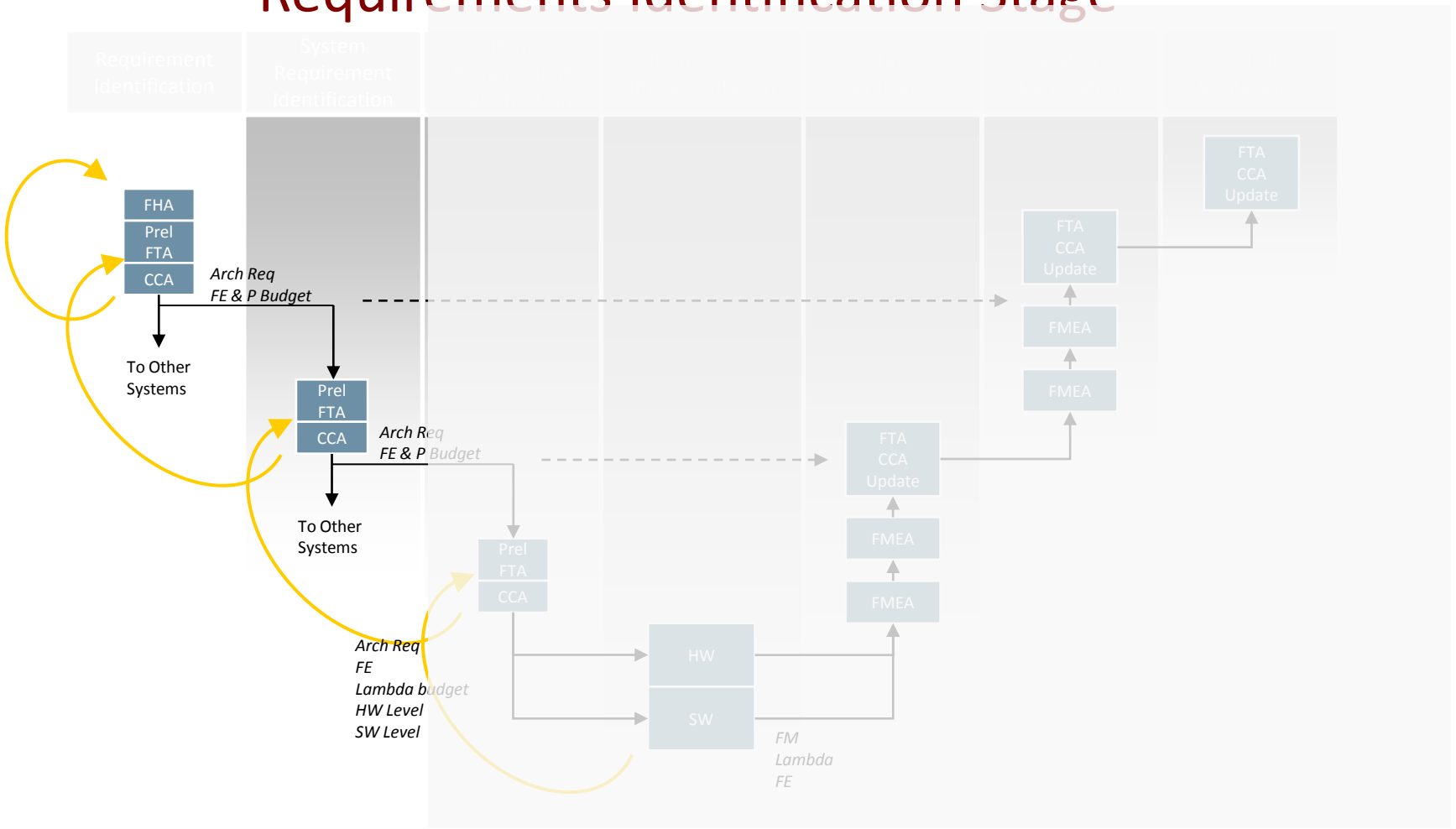


UPTIME®

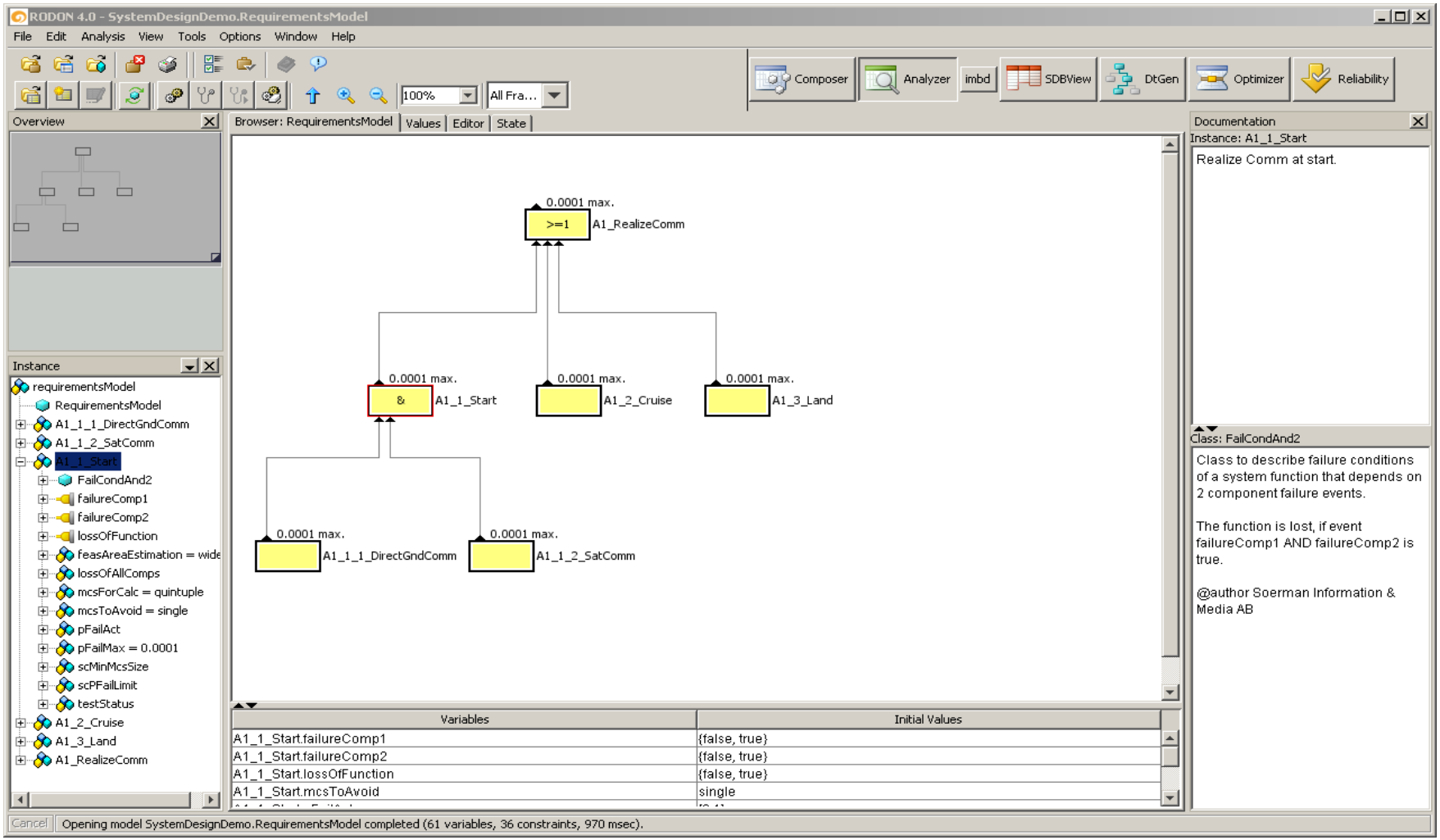
Diagnostics Results – Decision Trees



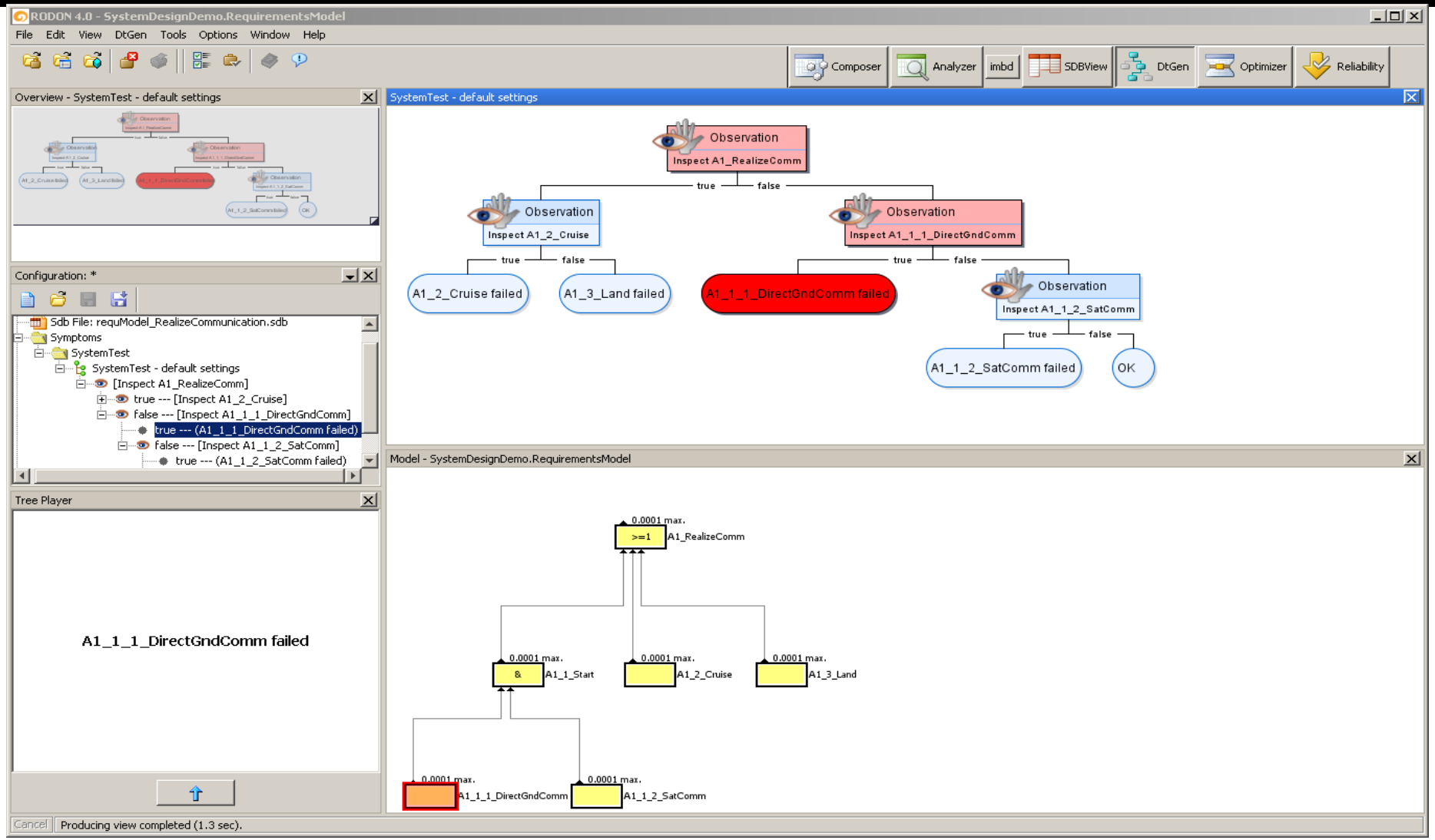
Requirements Identification Stage



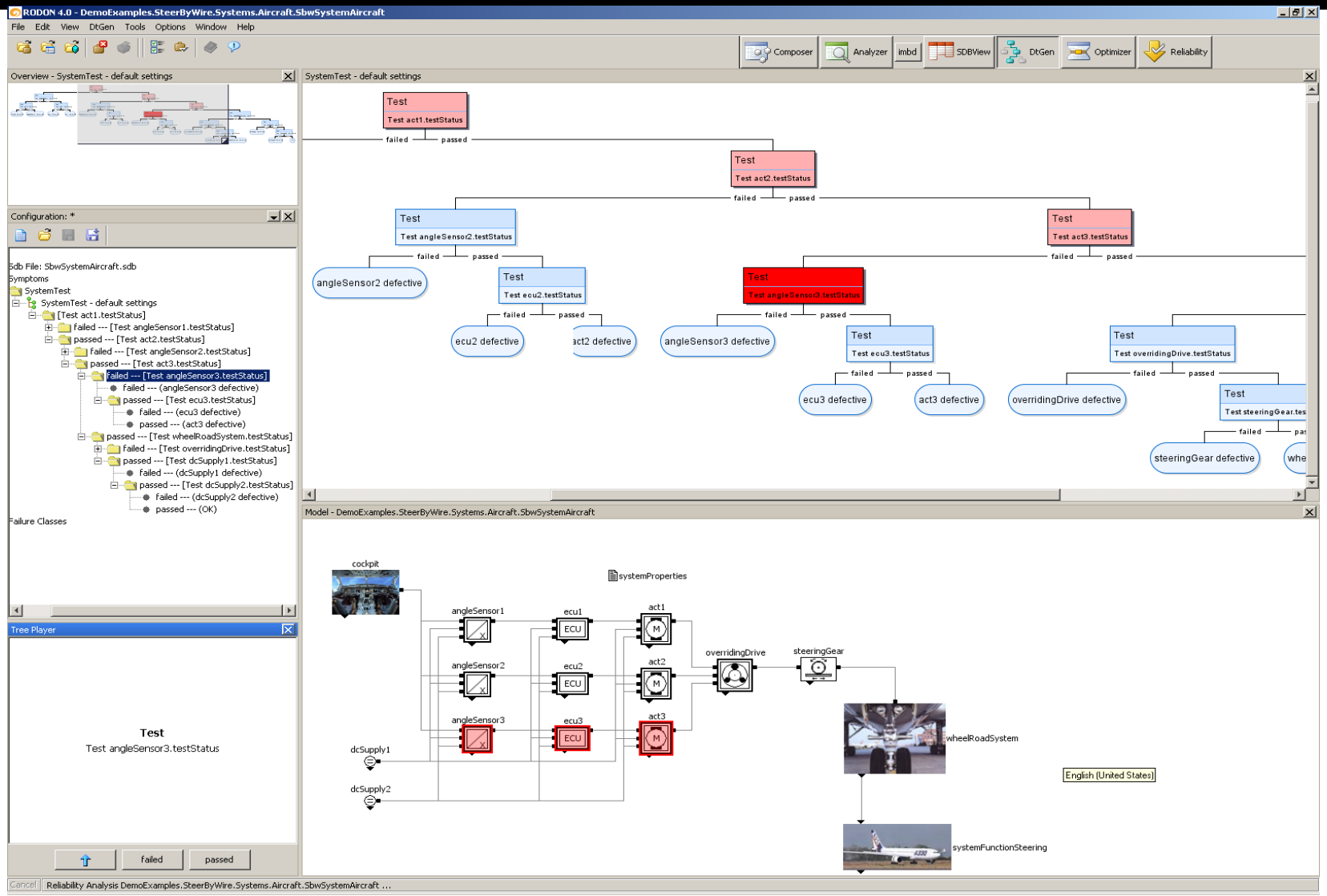
Early Function Failure Analysis



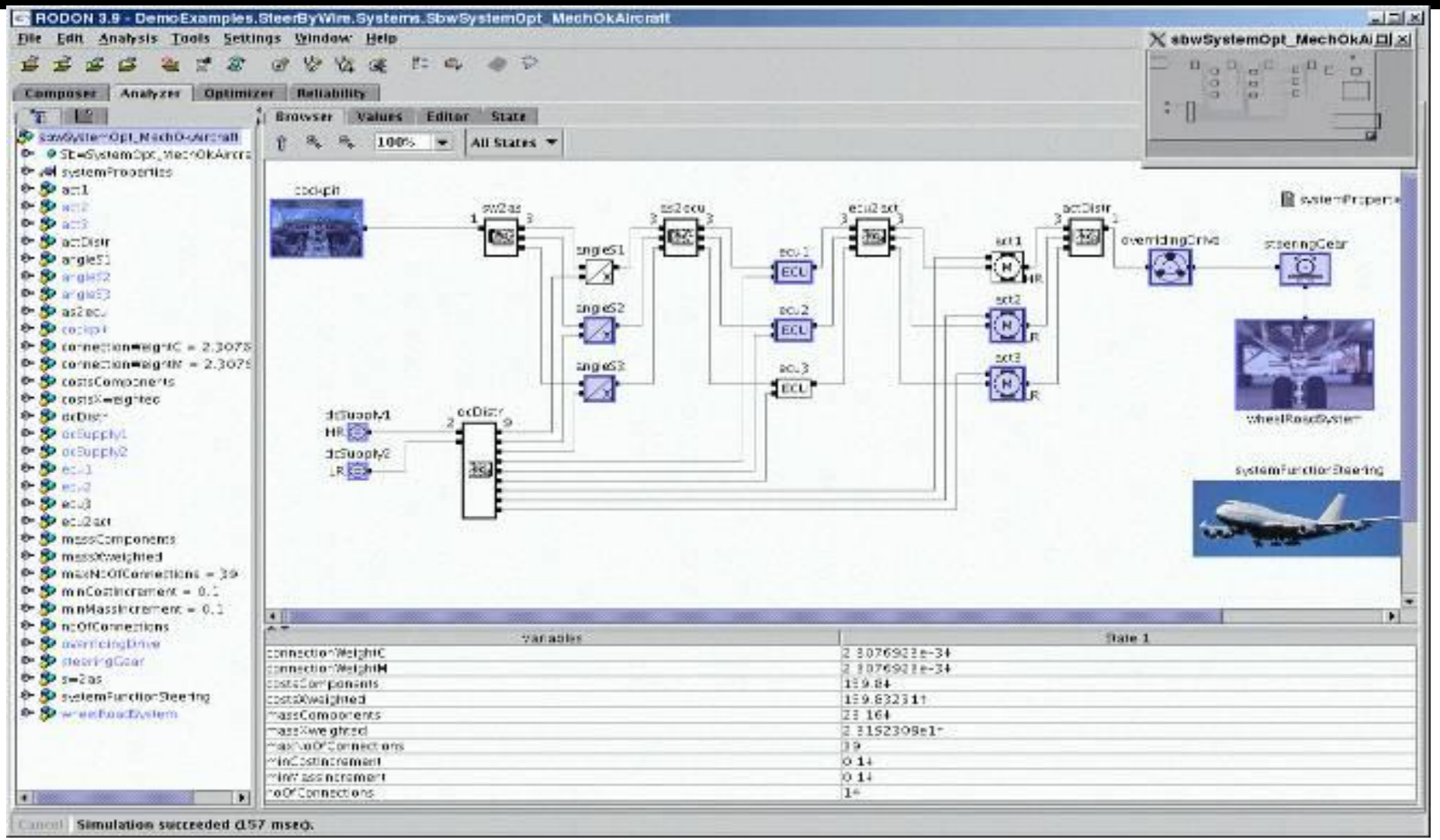
Early test strategies



Testability and Test Coverage



Models for Reliability Prediction

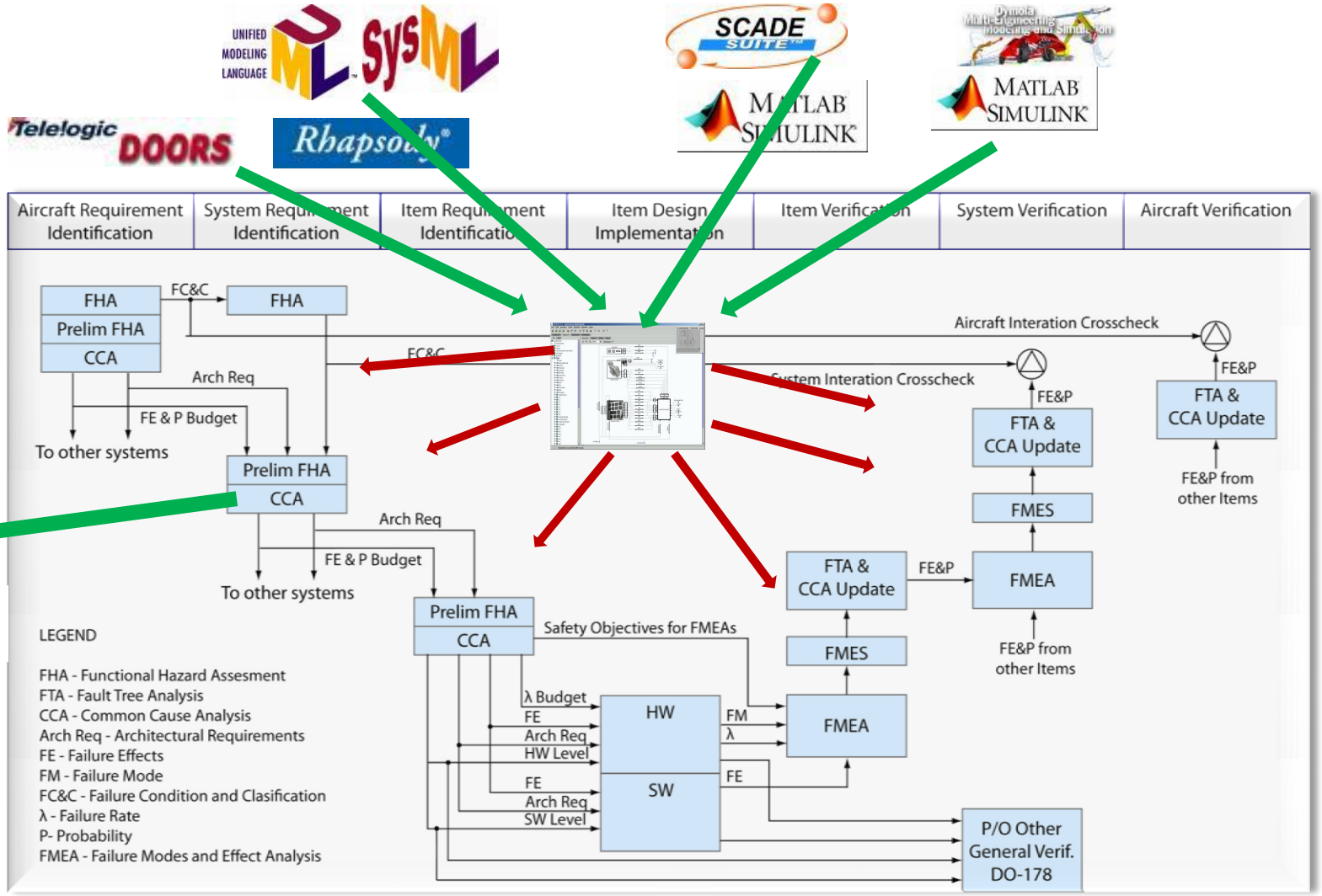


Model-Based Safety Assessment

- The biggest disadvantage of every model-based approach is the model itself
  - Building models takes time
  - Finding the right level of abstraction is difficult
- Model Reusability can be achieved by development of generic model libraries

Communication with other Systems

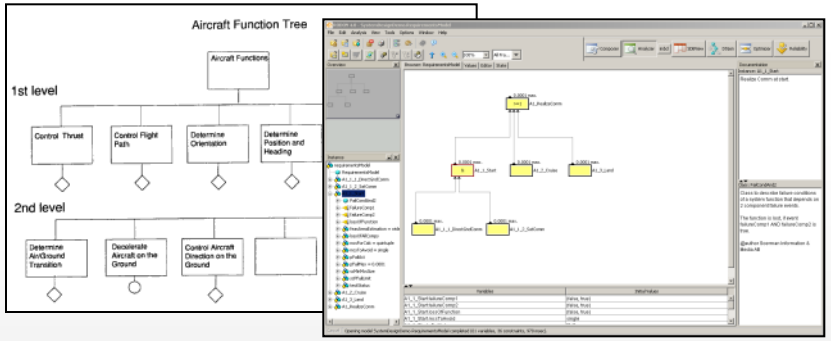
RELEX
ISOGRAPH
CFTA



Relex excellence in reliability

UPTIME®

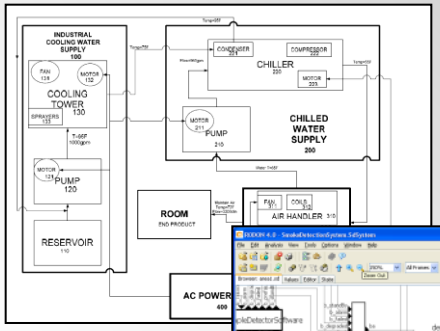
Modeling Challenge

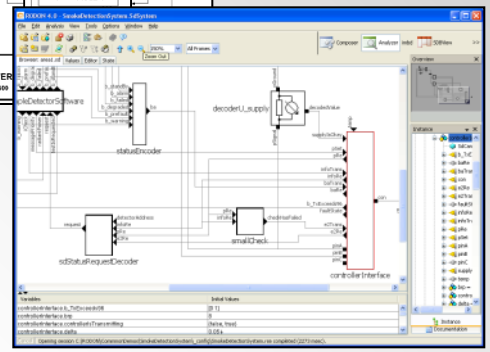


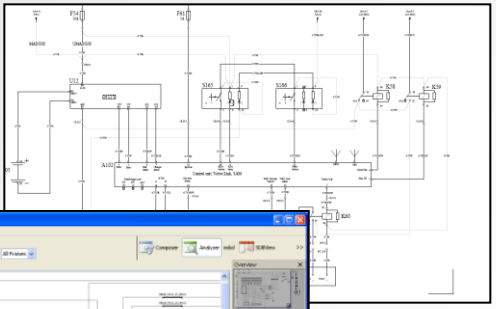
Failure Tree Analysis

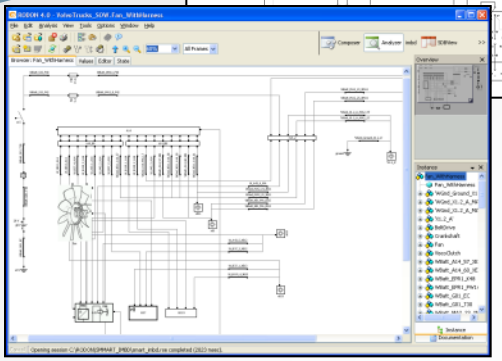
Function Architecture

System Architecture









Conclusions

- The Safety Assessment community should look closer on integrations issues as well
- Common modeling formalism and model-based approach for safety assessment process is important.