Towards a Conceptual Data Model for Fault Detection, Isolation and Recovery in Virtual Satellite

Sascha Müller (sa.mueller@dlr.de)

Agenda

1. What is FDIR
2. What is Virtual Satellite 4
3. FDIR Conceptual Data Model

Fault Detection, Isolation and Recovery in a Nutshell

Faults may occur in the System and turn into Failures if not handled

Doing FDIR means:

- **Detect** the occurrence of a fault
- **Isolate** the fault and localize it
- **Recover** the system

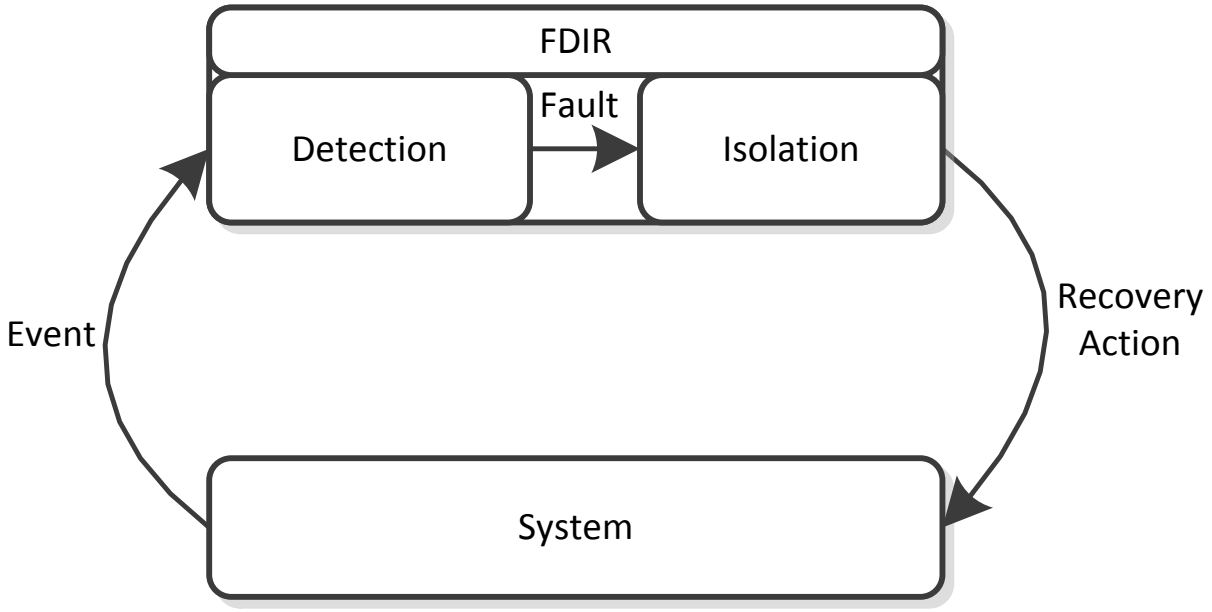


Fig: Relationship between System and FDIR

Quick intro into Virtual Satellite 4

- **Concurrent Engineering** framework
- Aiming to support **Model-Based Systems Engineering** for the **whole life cycle** of spacecraft
- Currently used in the **Concurrent Engineering Facility** at DLR

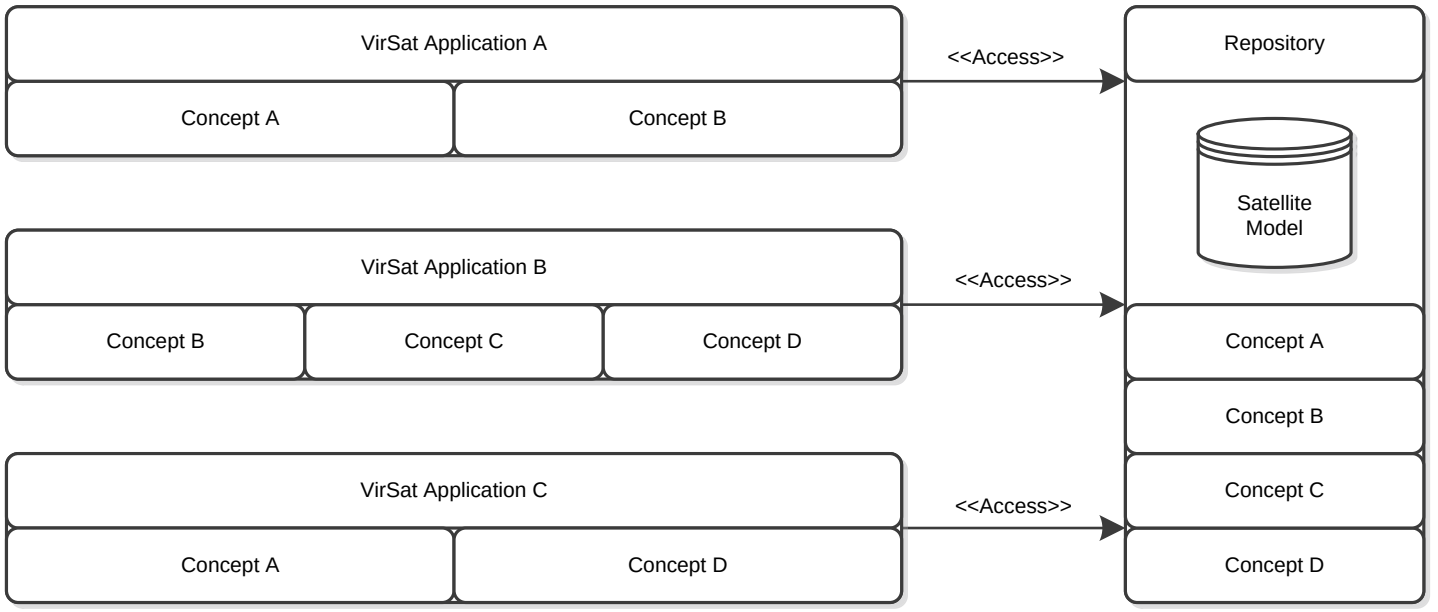


Fig: Virtual Satellite 4 architecture with extensions operating on the same repository

Conceptual Data Model

"data model that captures the end-user needs in the end-user terms" (ECSS-E-TM-10-23)

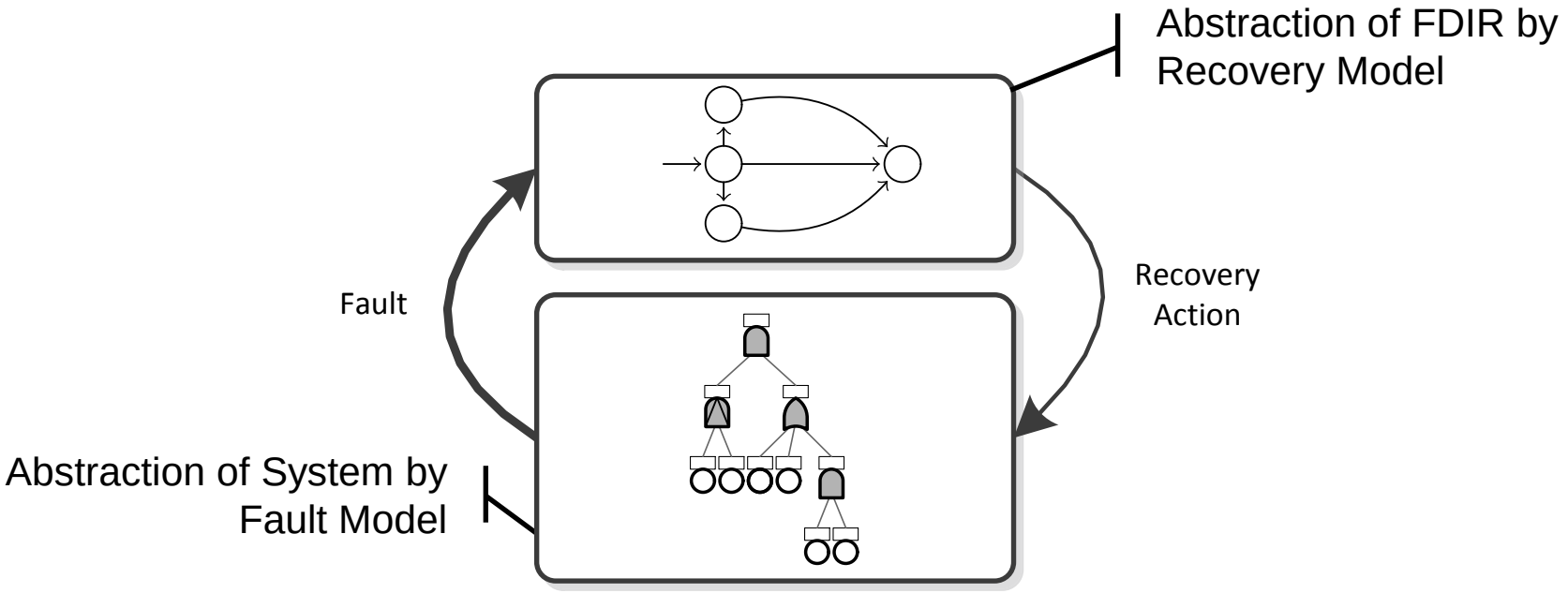


Fig: Model abstraction of System and FDIR

Model Evolution along Engineering Phases

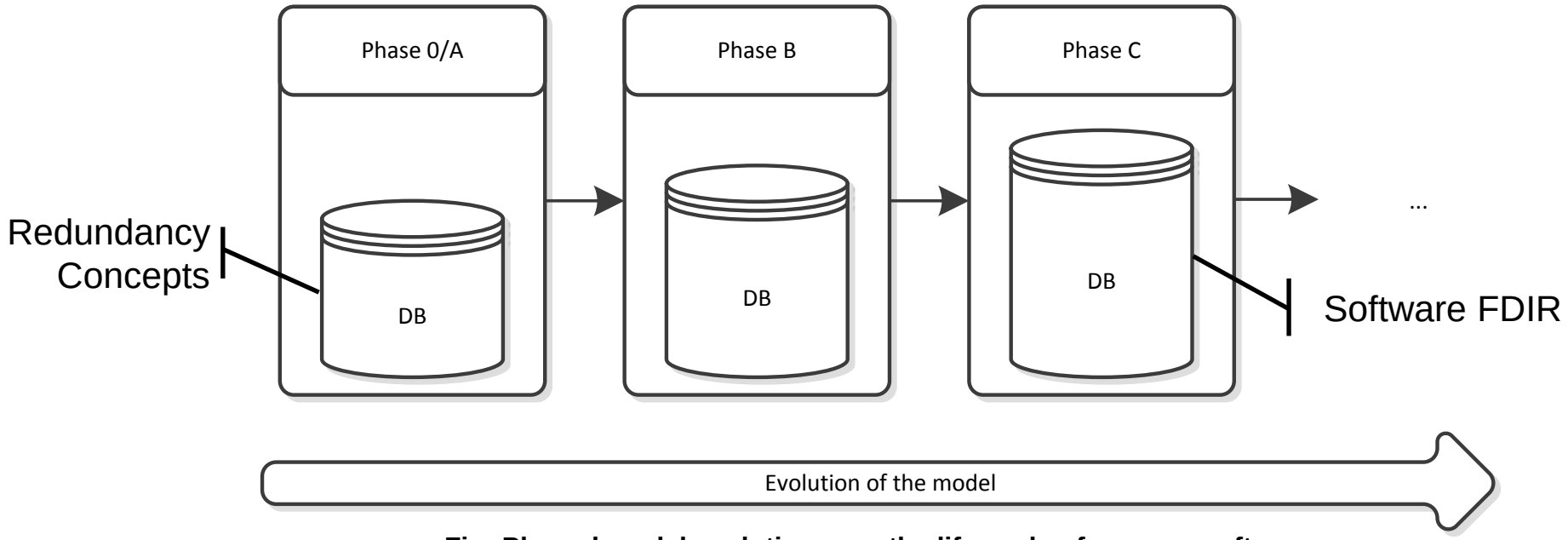


Fig: Phased model evolution over the life cycle of a spacecraft

Model Basic Systems Engineering for FDIR – The Challenges

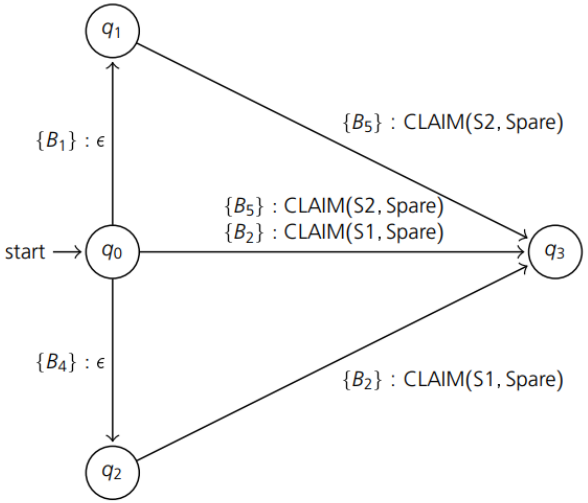
- **Extensibility**
  - Different domains, plugin new recovery actions
- **Model evolution**
  - Design focus shifts
- **Usefulness**
  - Model evaluation to deduce properties from
  - Verification & Validation

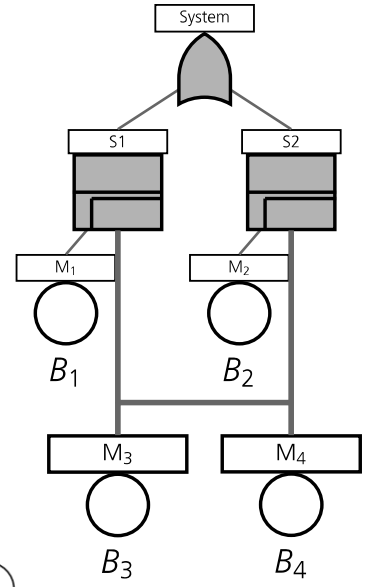
FDIR Conceptual Data Model

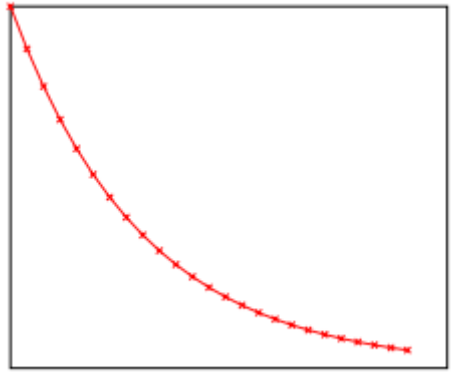
Three Main Ingredients:

- Fault Model
  - What can break?
- Recovery Model
  - How do we fix it?
- Requirements & Analysis Model
  - How do we validate it?

- **Future:** Detection Model







Fault Model

- **Fault Trees…**
  - capture wide array of information
  - remain computationally tractable

- **Answers question:** How do basic faults propagate and become system wide failures?

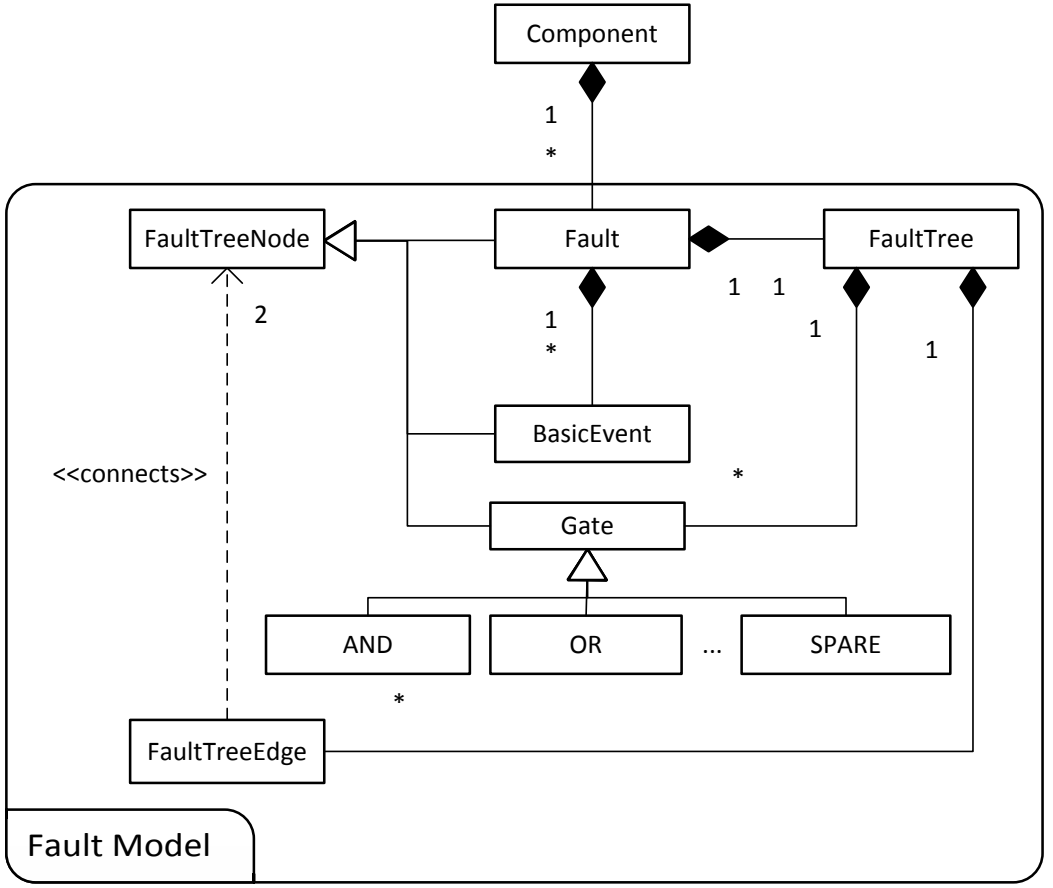


Fig: Representation of the Fault Model

Recovery Model

- Listens to output of fault model, returns recovery action
- Can extend and provide new Recovery Actions
- **Ongoing research:** Synthesizing Recovery model from fault model

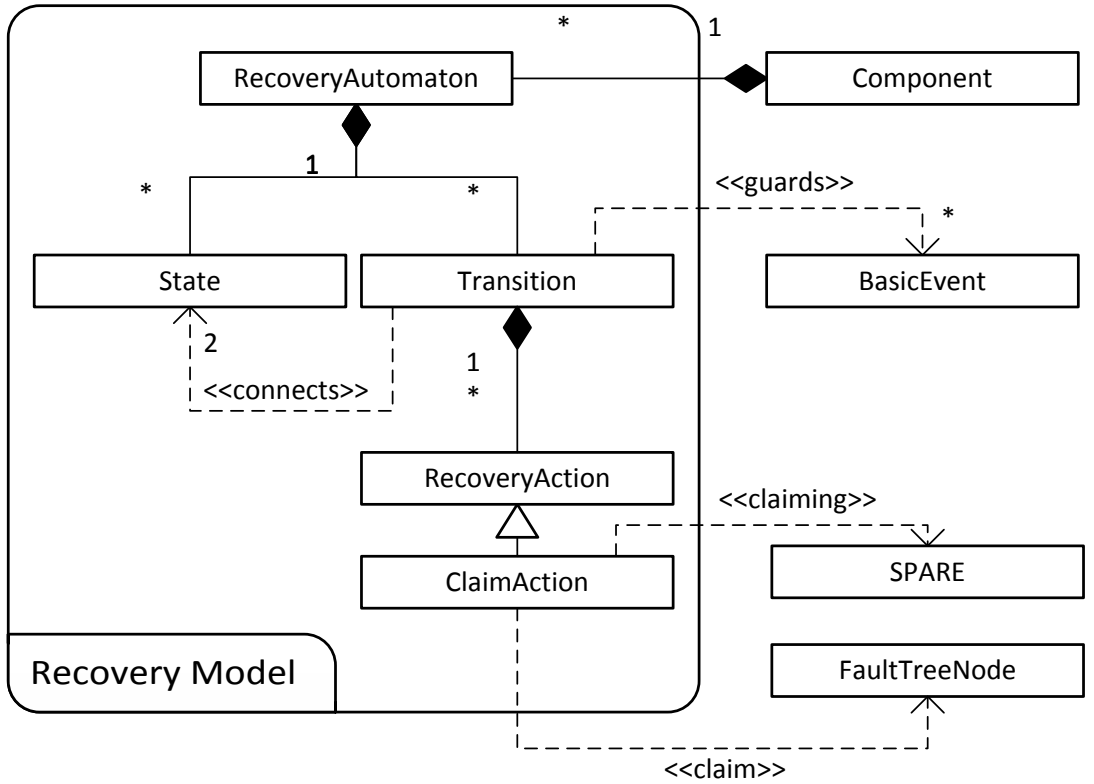


Fig: Representation of the Recovery Model

Analysis & Requirements Model

- Qualitative Analysis
  - **Requirement:** *“There is no single point of failure”*
  - **Analysis:** Fault Tolerance

- Quantitative Analysis
  - **Requirement:** *„The spacecraft can survive for 2 years with high probability“*
  - **Analysis:** Reliability

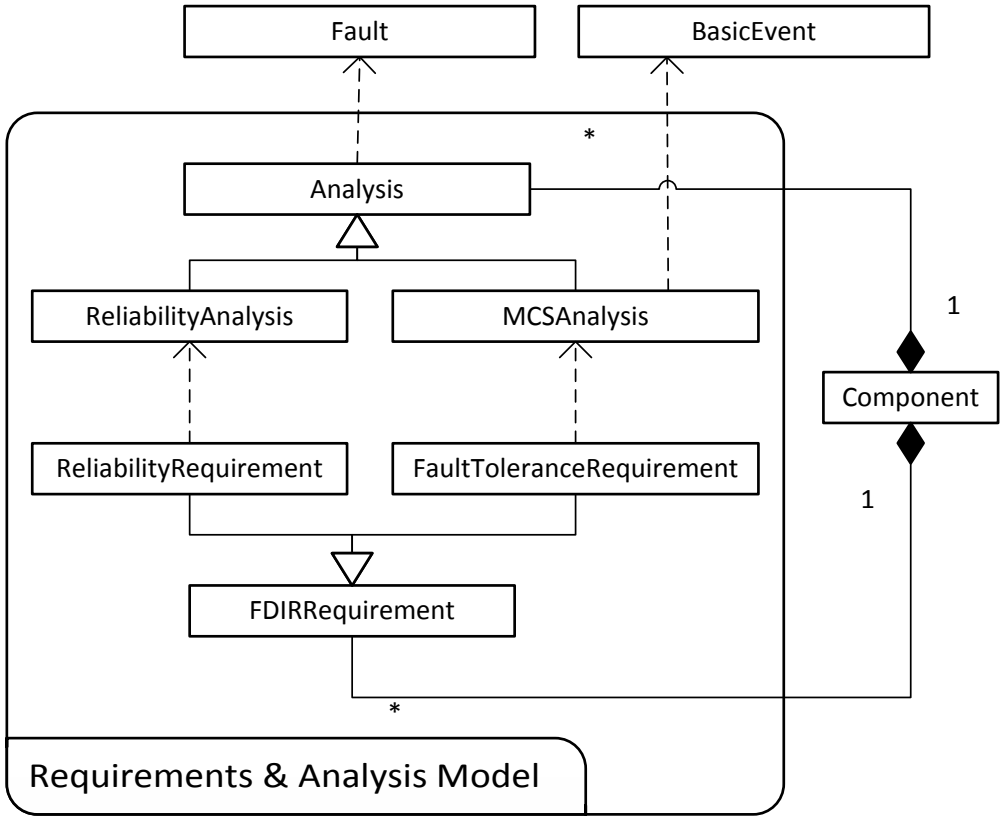


Fig: Representation of the Analysis & Requirements Model

VirSat FDIR

- Currently realizing approach in tool **VirSat FDIR**
- Virtual Satellite 4 application equipped with Conceptual Data Model for FDIR
- Annotation of equipment with Fault, Recovery and Analysis information

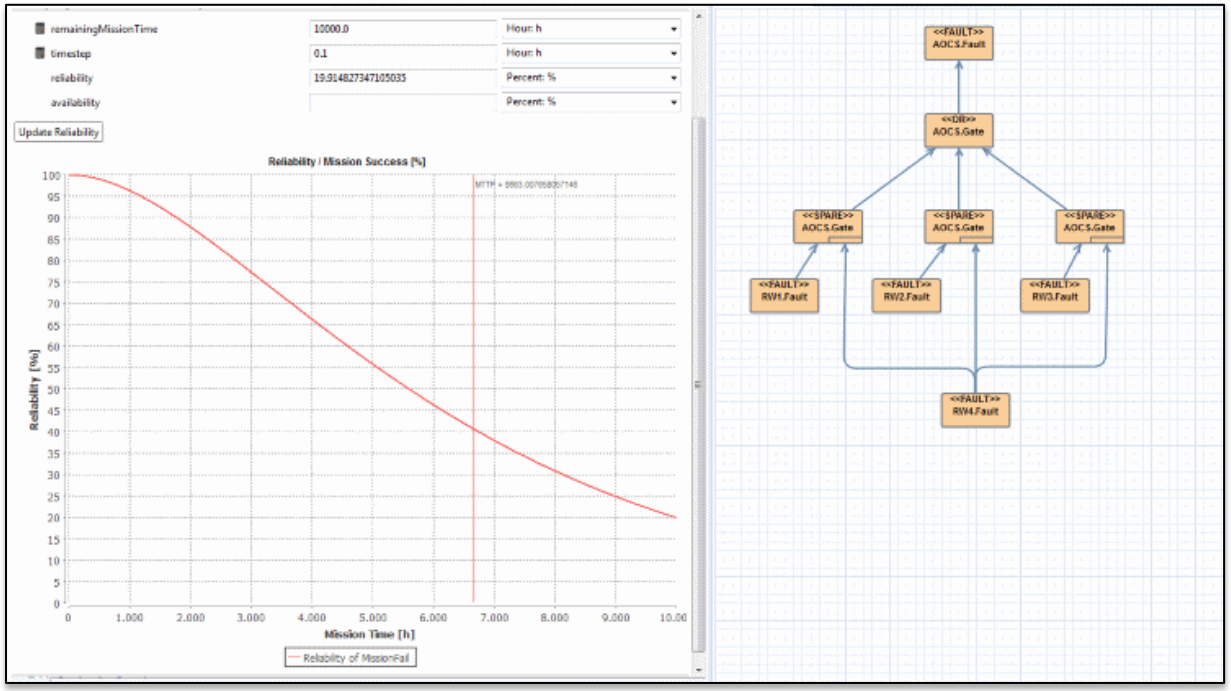


Fig: Screenshot of VirSat FDIR

Thank You!!