Synthesizing FDIR Recovery Strategies

Safety of Future Systems Workshop 2018

Sascha Müller
DLR German Aerospace Center
Institute of Simulation and Software Technology
Software for Space Systems and Interactive Visualization
Braunschweig

April 9 - 13

Knowledge for Tomorrow

DLR

Fault Detection, Isolation and Recovery

FDIR

Even well designed systems cannot avoid the existence of faults

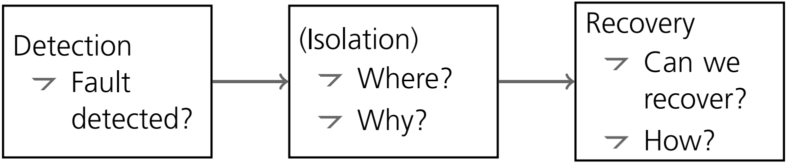
- But not every fault is a **failure**
- FDIR tries to prevent faults from turning into failures

Fault Detection, Isolation and Recovery

FDIR

Even well designed systems cannot avoid the existence of faults

- But not every fault is a **failure**
- FDIR tries to prevent faults from turning into failures



Detection

- Fault detected?

(Isolation)

- Where?
- Why?

Recovery

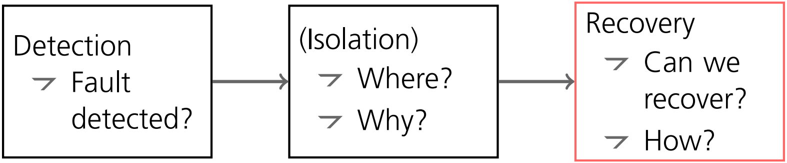
- Can we recover?
- How?

Fault Detection, Isolation and Recovery

FDIR

Even well designed systems cannot avoid the existence of faults

- But not every fault is a **failure**
- FDIR tries to prevent faults from turning into failures



Detection
- Fault detected?

(Isolation)
- Where?
- Why?

Recovery
- Can we recover?
- How?

Modeling the F in FDIR

Fault Model

Relationship between basic faults and how they lead to failures

- **Fault Tree Analysis**
- Failure Modes and Effects Analysis
- ... and many more

Modeling the F in FDIR

Fault Model

Relationship between basic faults and how they lead to failures

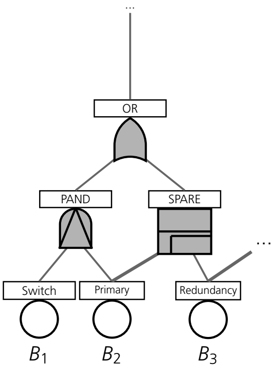
- **Fault Tree Analysis**
- Failure Modes and Effects Analysis
- ... and many more

Problem

Input: Given a fault model...

Output: ...compute a Recovery Strategy.

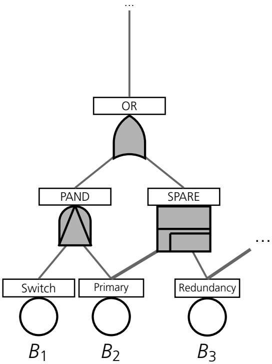
Dynamic Fault Trees - Spare Gate

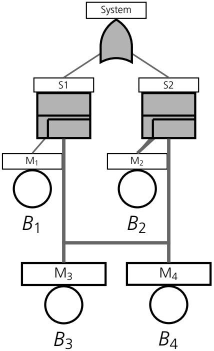


Issues with default semantics

- Order is statically fixed
- Spare order may not be optimal
- Semantic issues with concurrent spare claims

Dynamic Fault Trees - Spare Gate





Issues with default semantics

- Order is statically fixed
- Spare order may not be optimal
- Semantic issues with concurrent spare claims

Non-Deterministic Fault Trees

Idea

Split Fault Tree up into...

- Non-Deterministic Fault Tree (NdDFT)
  - No Fixed spare ordering
- Deterministic Recovery Strategy (Recovery Automaton)
  - Recovery actions: Claim spare gate, do nothing

Non-Deterministic Fault Trees

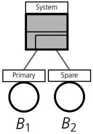
Idea

Split Fault Tree up into...

- Non-Deterministic Fault Tree (NdDFT)
  - No Fixed spare ordering
- Deterministic Recovery Strategy (Recovery Automaton)
  - Recovery actions: Claim spare gate, do nothing

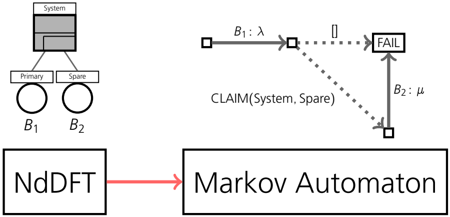
Encode nondeterministic decision for applying recovery actions in a Markov Automaton model.

Transformation Road Map

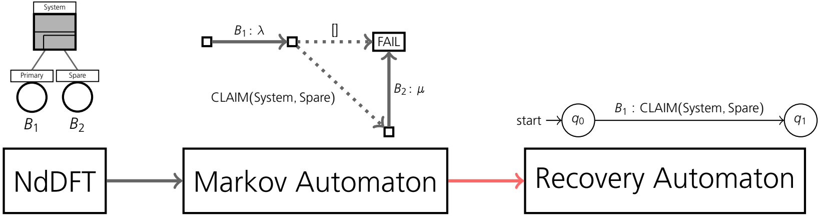


NdDFT

Transformation Road Map



Transformation Road Map

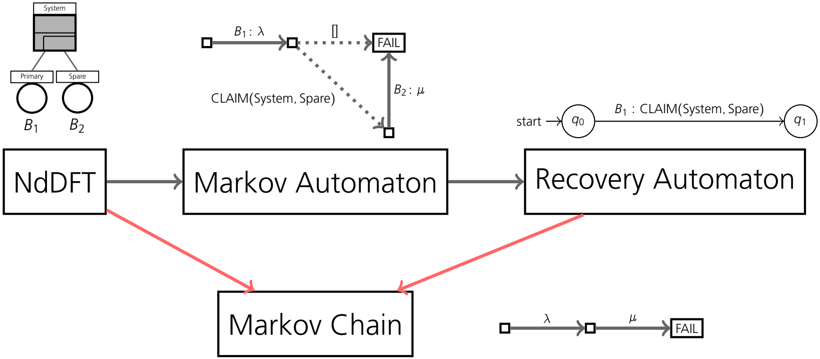


NdDFT

Markov Automaton

Recovery Automaton

Transformation Road Map



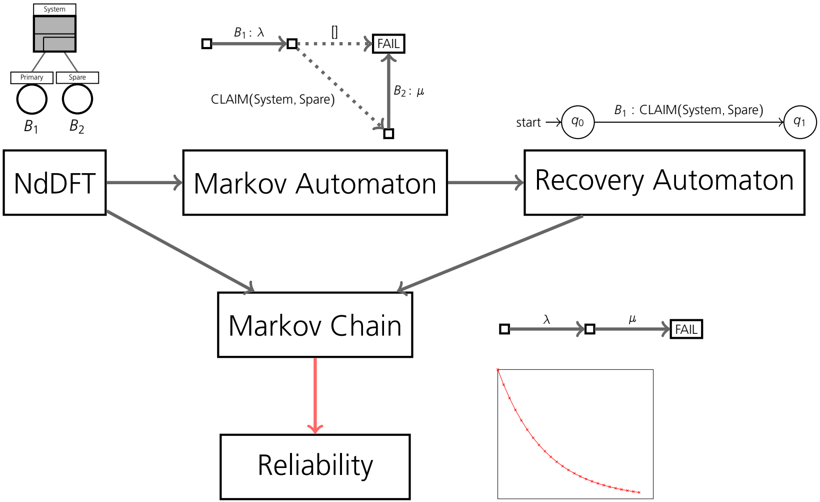
NdDFT

Markov Automaton

Recovery Automaton

Markov Chain

Transformation Road Map



NdDFT

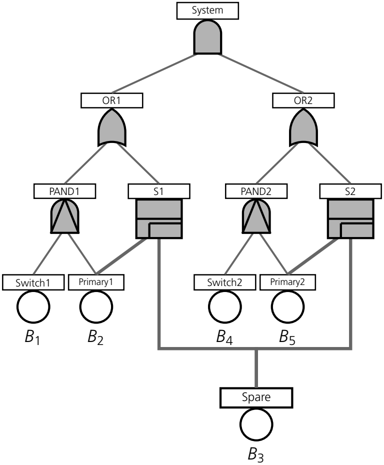
Markov Automaton

Recovery Automaton

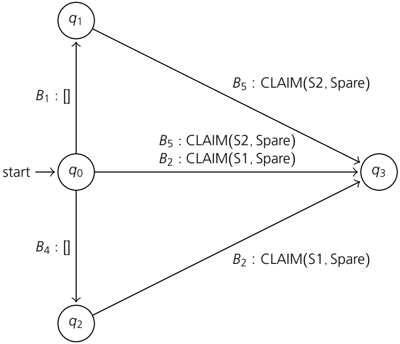
Markov Chain

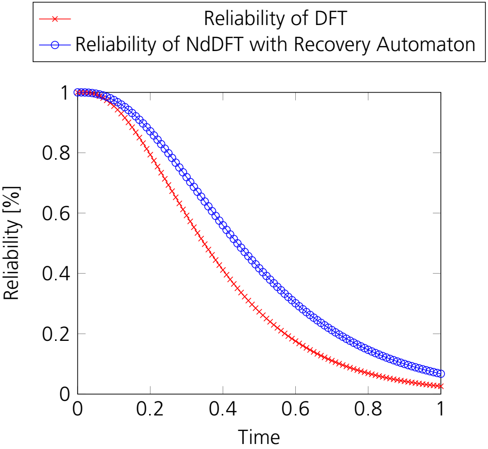
Reliability

Example


System
OR1
OR2
PAND1
S1
PAND2
S2
Switch1
Primary1
Switch2
Primary2
B_1
B_2
B_4
B_5
Spare
B_3

Example - Results





Formalization of Recovery Actions

Future...

Other actions that are relevant:

- Repair
  ("Reset failed sensor")

Formalization of Recovery Actions

Future...

Other actions that are relevant:

- Repair
  ("Reset failed sensor")
- **Mode changes**
  ("Switch to Safe Mode")

Formalization of Recovery Actions

Future...

Other actions that are relevant:

- Repair
  ("Reset failed sensor")
- **Mode changes**
  ("Switch to Safe Mode")
- Maintenance
  ("Flush memory to clean data corruptions")

Thank You!!