iFM & ABZ 2012 Tutorial
Safety, Dependability and Performance Analysis of Extended AADL Models
Part 5: Fault Detection, Isolation and Recovery Analysis

European Space Agency
European Space Research and Technology Centre

RWTH Aachen University
Software Modeling and Verification Group
Joost-Pieter Katoen & Thomas Noll

Fondazione Bruno Kessler
Centre for Scientific and Technological Research
Marco Bozzano & Alessandro Cimatti

iFM & ABZ 2012; June 18, 2012; Pisa, Italy

Outline

Fault Detection, Isolation and Recovery

FDIR

- The FDIR (Fault Detection, Isolation and Recovery) sub-system is an essential block of safety-critical systems
- It runs online, in parallel with the system
- The FDIR block must be able to detect malfunctions, and carry out suitable reactions
- Needed to ensure fault tolerance of the system, and prevent the occurrence of safety hazards

Fault Detection, Isolation and Recovery

FDIR

- The FDIR (Fault Detection, Isolation and Recovery) sub-system is an essential block of safety-critical systems
- It runs online, in parallel with the system
- The FDIR block must be able to detect malfunctions, and carry out suitable reactions
- Needed to ensure fault tolerance of the system, and prevent the occurrence of safety hazards

Goals of FDIR

- Fault detection: identify malfunctions
- Fault isolation: precisely identify the fault responsible for a malfunction
- Fault recovery: recover after a fault has occurred, e.g. reconfiguring the system or switching operational mode

Outline

FDIR Analyses

FDIR Effectiveness Analysis

- Evaluate the effectiveness of an existing diagnoser. It includes:
  - Fault Detection Analysis
  - Fault Isolation Analysis
  - Fault Recovery Analysis

FDIR Analyses

FDIR Effectiveness Analysis

- Evaluate the effectiveness of an existing diagnoser. It includes:
  - Fault Detection Analysis
  - Fault Isolation Analysis
  - Fault Recovery Analysis

Diagnosability Analysis

- Check if there exists a diagnoser that can infer at run-time accurate and sufficient information on the behavior of the plant

FDIR Analyses

FDIR Effectiveness Analysis

- Evaluate the effectiveness of an existing diagnoser. It includes:
  - Fault Detection Analysis
  - Fault Isolation Analysis
  - Fault Recovery Analysis

Diagnosability Analysis

- Check if there exists a diagnoser that can infer at run-time accurate and sufficient information on the behavior of the plant

Goals of FDIR Analyses

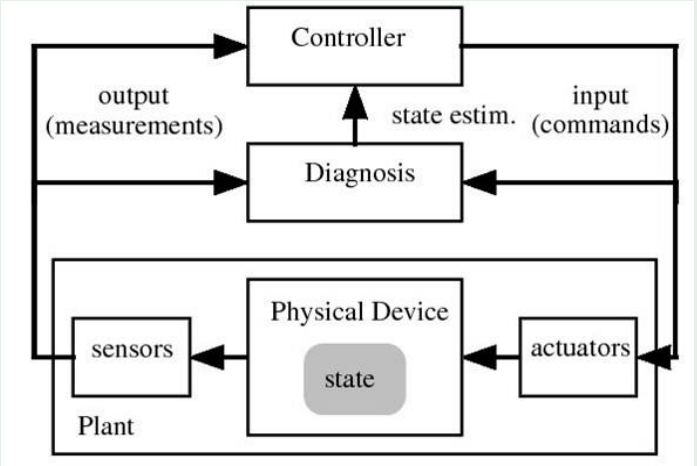
- Both analyses are carried out offline (on ground)
  - FDIR effectiveness analysis evaluates the capabilities of an implemented FDIR sub-system
  - Diagnosability analysis helps identifying if enough observables are available for building an FDIR sub-system

FDIR Context

Diagnosis system

- Plant (Physical Device) in closed loop with a controller
- Controller is responsible for commanding actuators
- Diagnosis system tracks the hidden state of the plant over time

Diagnosis

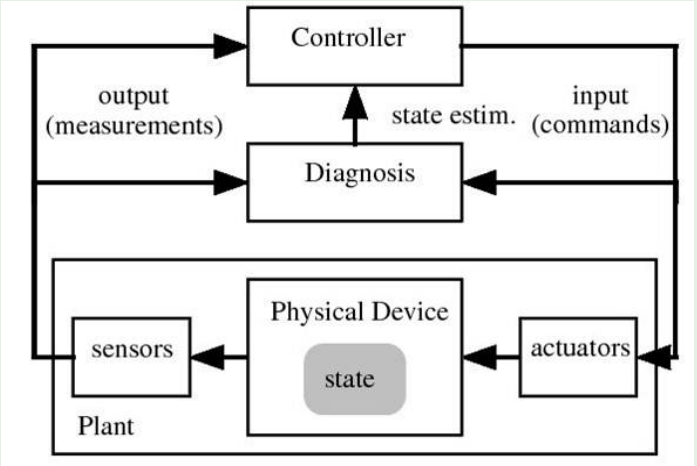


FDIR Context

Diagnosis system

- Plant (Physical Device) in closed loop with a controller
- Controller is responsible for commanding actuators
- Diagnosis system tracks the hidden state of the plant over time

Diagnosis



Diagnosis assumptions

- Partial observability: only a limited number of observables (e.g., sensors) can be monitored
- Passive diagnosis: diagnosis system cannot issue commands to the plant, in order to carry out diagnosis

Fault Detection Analysis

Fault Detection

- Evaluates capabilities of an existing FDIR sub-system to detect faults
- Answers the question: "Is it always possible to detect a fault?"

Fault Detection Analysis

Fault Detection

- Evaluates capabilities of an existing FDIR sub-system to detect faults
- Answers the question: "Is it always possible to detect a fault?"

Fault Detection in COMPASS

- It can be reduced to a model checking problem
- Given a fault F and an observable O: "Is it always the case that occurrence of F will eventually trigger O?"
- Observable O is called a detection means for fault F
- COMPASS can synthesize all such observables, for any given fault.
- Detection means are alarms triggered by the FDIR sub-system

Fault Isolation Analysis

Fault Isolation

- Evaluates capabilities of an existing FDIR-sub-system to identify faults
- In general, when an anomaly is detected, it may be impossible to precisely identify the responsible fault
- Answers the question: "Which faults are possible explanations for an event?"
- Perfect isolation: only one fault is identified as possible explanation

Fault Isolation Analysis

Fault Isolation

- Evaluates capabilities of an existing FDIR-sub-system to identify faults
- In general, when an anomaly is detected, it may be impossible to precisely identify the responsible fault
- Answers the question: "Which faults are possible explanations for an event?"
- Perfect isolation: only one fault is identified as possible explanation

Fault Isolation in COMPASS

- It can be reduced to a fault tree generation problem
- Given a set of observable events O, generate a fault tree for each $o \in O$, representing the possible explanations for o
- Perfect isolation corresponds to a fault tree with only one MCS (or order 1)

Fault Recovery Analysis

Fault Recovery

- Evaluates capabilities of an existing FDIR sub-system to recover from faults
- Answers the question: "Is it always possible to recover from a fault?"

Fault Recovery Analysis

Fault Recovery

- Evaluates capabilities of an existing FDIR sub-system to recover from faults
- Answers the question: "Is it always possible to recover from a fault?"

Fault Recovery in COMPASS

- It can be reduced to a model checking problem
- A recoverability property can be specified by the user
- Fully general properties can be expressed
- E.g.: given a fault F and a condition P: "Is it always the case that whenever F occurs, eventually the system will satisfy condition P?"

Diagnosability Analysis

Plant

A plant is a tuple $P =< X, U, Y, \delta, \lambda >$, where:

- X is a finite set, called the state space
- $X_0 \subseteq X$ is the set of initial states
- U is a finite set, called the input space
- Y is a finite set, called the output space
- $\delta \subseteq X \times U \times X$ is the transition relation
- $\lambda \subseteq X \times Y$ is the observation relation

Diagnosability Analysis

Trace

A trace (feasible execution) of the plant, with a discrete number of time steps t, is as a sequence $\pi = \langle x^0, y^0, u^1, x^1, y^1, \ldots, u^t, x^t, y^t \rangle$ such that:

- $x^0 \in X_0$
- $\delta(x_{i-1}, u_i, x_i)$ for $i = 1, \ldots, t$
- $\lambda(x_i, y_i)$ for $i = 0, \ldots, t$

Diagnosability Analysis

Trace

A trace (feasible execution) of the plant, with a discrete number of time steps t, is as a sequence $\pi = \langle x^0, y^0, u^1, x^1, y^1, \ldots, u^t, x^t, y^t \rangle$ such that:

- $x^0 \in X_0$
- $\delta(x_{i-1}, u_i, x_i)$ for $i = 1, \ldots, t$
- $\lambda(x_i, y_i)$ for $i = 0, \ldots, t$

Observable Trace

The observable part of a trace consists of the input and output signal: $obs(\pi) = \langle y^0, u^1, y^1, \ldots, u^t, y^t \rangle$

Diagnosability Analysis

Diagnosis condition

A diagnosis condition for a a plant P is a pair of nonempty and disjoint sets of states $c_1, c_2 \subseteq X$, written $c_1 \perp c_2$

Diagnosability Analysis

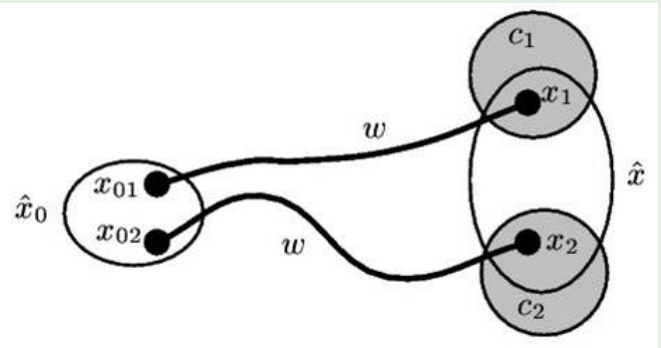
Diagnosis condition

A diagnosis condition for a a plant P is a pair of nonempty and disjoint sets of states $c_1, c_2 \subseteq X$, written $c_1 \perp c_2$

Critical Pair

A critical pair for diagnosis condition $c_1 \perp c_2$ and delay d, given plant P, is a pair of system traces π_1 and π_2, both of length $t + d$, with the same observable traces w, such that $x^t_{\pi_1} \in c_1 \wedge x^t_{\pi_2} \in c_2$ holds

Critical Pair



Diagnosability Analysis

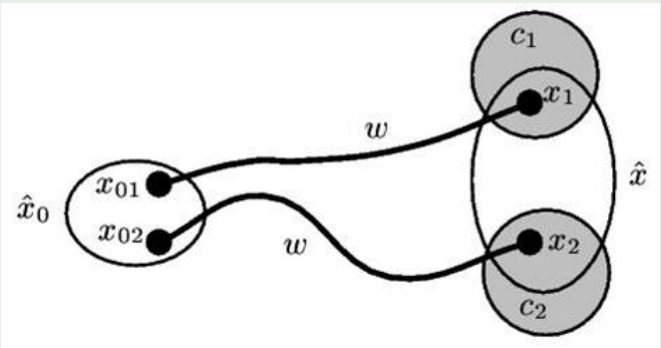
Diagnosis condition

A diagnosis condition for a a plant P is a pair of nonempty and disjoint sets of states $c_1, c_2 \subseteq X$, written $c_1 \perp c_2$

Critical Pair

A critical pair for diagnosis condition $c_1 \perp c_2$ and delay d, given plant P, is a pair of system traces π_1 and π_2, both of length $t + d$, with the same observable traces w, such that $x^t_{\pi_1} \in c_1 \wedge x^t_{\pi_2} \in c_2$ holds

Critical Pair



Diagnosability in COMPASS

- A plant is diagnosable is there exists no critical pair, that is, a pair of traces, one "good" and one "bad", that are indistinguishable
- Diagnosability can be reduced to a model checking problem using the so-called twin-plant construction

References

- Diagnosability and Twin-Plant (Cimatti et. al, IJCAI 2003)
- Synthesis of Observability Requirements (Bittner et. al, AAAI 2012)
- Synthesis of FDIR (Alaña et. al, DASIA 2012)

Outline

Ongoing Activities

FDIR Synthesis

- New ESA study: AUTOGEF
- Automated synthesis of an FDIR sub-system starting from a set of FDIR requirements, including:
  - Architectural constraints (centralized vs distributed FDIR)
  - Detection, Isolation and Recovery requirements
  - Performance requirements

Ongoing Activities

FDIR Development Lifecycle

- New ESA study (under negotiation): FAME
- Dedicated FDIR Development Methodology and V&V Process:
  - Formal specification and analysis techniques
  - Integration of inputs from Mission, System Analysis and Specification, System and Software Development
- Integrated framework implementing the methodology and process
- Based on COMPASS (and AUTOGEF)

Outline

Content of Tool Demo

Demo Steps

1. Fault Detection Analysis
2. Fault Isolation Analysis
3. Fault Recovery Analysis