Raisonnement diagnostic pour la maintenance et l'autonomie de systèmes embarqués : un bref état et quelques défis

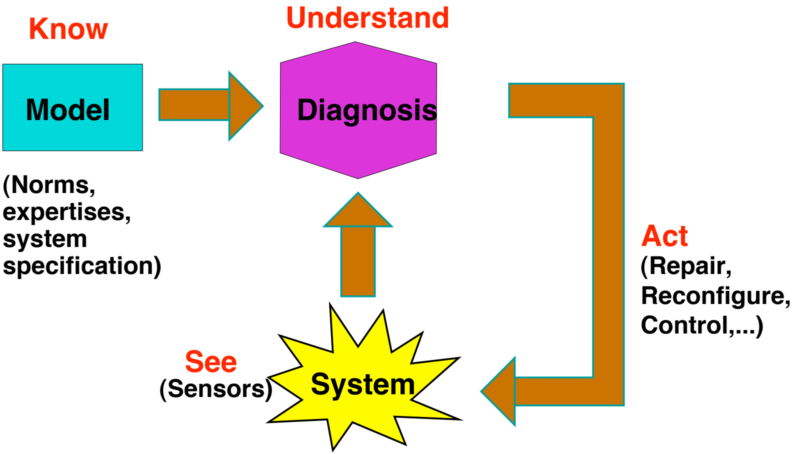
Yannick Pencolé

Workshop Mocosy

27 mars 2009

A very brief overview of model-based diagnosis and diagnosability: my starting point

Diagnosis principles



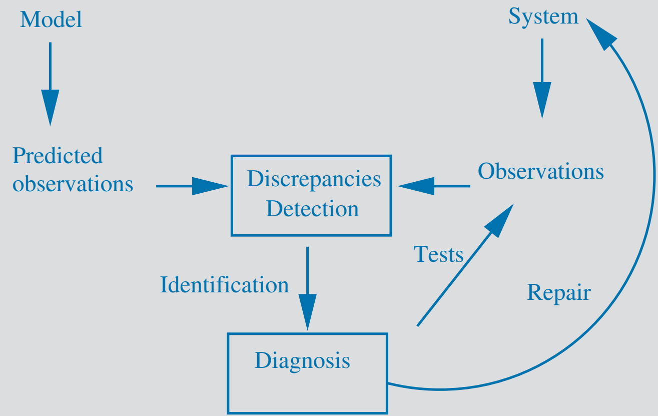
Diagnosis: history

History

- 70's: heuristic approaches (expert systems)
  - knowledge base = set of abductive rules (need expertise)
  - inference
- 80's: model-based diagnosis (static systems)
- 90's: model-based diagnosis (dynamic systems)
- 00's: diagnosability checking
- Present: design for diagnosability

Model-based diagnosis: the idea

Model-based diagnosis



Diagnosis: a basic introduction (static systems)

Definition

A system is a couple $(SD, COMP)$:

- $COMP$ is a finite set of constants, one constant = one component
- SD is a set of first-order logic sentences describing the behavioural modes $\mathscr{F}$ of $COMP$ of the system
  - Behavioural model (how a component works)
  - Structural model (how components interact)

Definition

A observed system is a system $(SD, COMP)$ with some observations OBS:

- OBS is a set of atomic sentences.
- Each atomic sentence represents an observation

Diagnosis: logical definition

Definition

A State of the system $SD, COMP$ is a sentence Φ like:

$$\Phi \equiv \bigwedge Mode(c, f)$$

A diagnosis candidate (hypothesis, accusation) of the system $SD, COMP$ is a state Φ such that:

$$SD \wedge OBS_{cons} \wedge \Phi \models OBS_{Abd} \text{ is satisfiable.}$$

The state Φ is possible according to SD, OBS_{cons} (consistency-based) and logically explains the symptoms OBS_{Abd} (root causes).

$$\Delta(SD, COMP, OBS_{cons} \wedge OBS_{Abd}) = \bigcup \{\Phi\}$$

$|\Delta| > 1$: ambiguous diagnosis

Towards dynamic systems

- Taking into account the notion of time, of change
  - Fault are not supposed to be present at diagnosis time
  - Fault occurrence during the diagnostic process
  - Problem of diagnosis and monitoring
- Use of other formalisms
  - Discrete-event systems
    - Model of the instantaneous changes of a system

On-line diagnosis

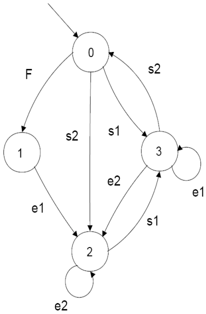
- On-line acquisition of observations
  - Monitoring
- Diagnostic updates (refinements) relying on a new set of observations: incremental diagnosis
  - $\Delta(SD, COMP, OBS_t) \rightarrow \Delta(SD, COMP, OBS'_t), t' > t$
- Diagnosis computation performed on a temporal window
- Efficiency requirements to “follow” the observation flow
- More compatible with an embedded system requirements

DES framework

- Model of a component: an automaton Γ_i
- Model of the system $\Gamma = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_n\}$
- Model of a subsystem $\gamma \subseteq \Gamma$, $\gamma \neq \emptyset$

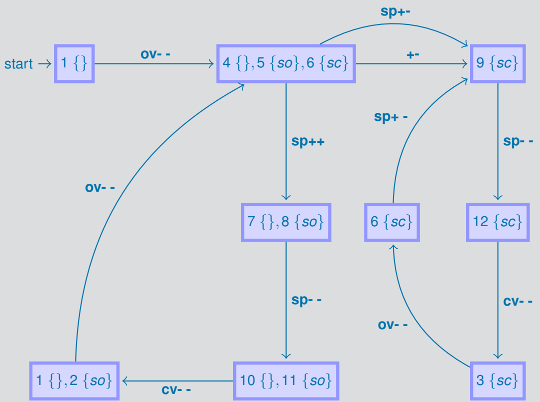
Model of a component: $\Gamma_i = (Q_i, \Sigma_i, T_i, q_{0i})$

- Q_i finite set of states
- Σ_i, set of events (local,communication) occurring on Γ_i
- $T_i \subseteq Q_i \times \Sigma_i \times Q_i$, set of transitions
- q_{0i}, initial state



$\Sigma_{oi} \subset \Sigma_i$ (observable), $\Sigma_i \subseteq \Sigma_i$ (fault)
$Mode(\Gamma_i, f) \equiv$ "The event f has occurred on Γ_i"

Classical diagnoser on a controller+pump+valve system



State $7\{\}, 8\{so\} \equiv Mode(controller, normal) \wedge Mode(pump, normal) \wedge (Mode(valve, normal) \vee Mode(valve, so))$

Diagnosability in a DES

In pratice, given a flow of observations *OBS* at time *t*,
two cases hold:

1. $|\Delta(SD, OBS)| = 1$: non-ambuiguity
2. $|\Delta(SD, OBS)| > 1$: ambiguity

Definition

Event *F* is diagnosable if it is always possible to diagnose its occurrence with certainty after a finite number of observations that follow the occurrence of *F*.

In other words, *F* is diagnosable:

1. It is always possible to decide about the occurrence of *F*
2. This decision is done after waiting for a finite set of observations

Diagnosis for maintenance and autonomy in embedded systems: my objectives

Notion of embedded system

Definition

An embedded system is an engineering artifact involving computation that is subject to physical constraints. The physical constraints arise through the two ways that computational processes interact with the physical world:

1. reaction to a physical environment
2. execution on a physical platform.

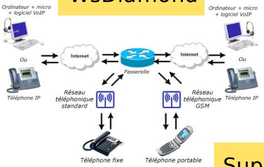
T.A. Henzinger and J. Sifakis. The Discipline of Embedded Systems Design, Computer, October 2007, pp. 32-40.

Characteristics of embedded systems

- Dynamic systems
- Component-based systems (compositional design)
- Reasoning capabilites but limited computational ressources
- Heterogenous components (electronic, hydraulic, mechanic,...)
- Action capabilities

Embedded systems from my project involvements

WsDiamond

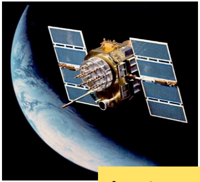


Supercom

Diagnosis in embedded systems:

Why ?
How ?

Archistic



Agata

Rosace

Objectives

- Improving the maintenance of commercial embedded systems (aircrafts, cars, “robots”)
  - Repair what is broken in the system.
- Improving the autonomy of embedded systems (robots, satellites)
  - Act in order to achieve the goals whatever the difficulties are.

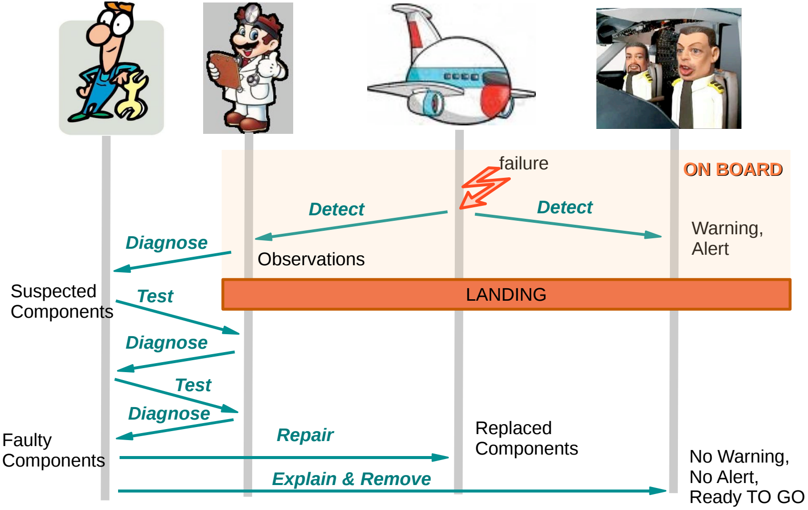
Objectives:

How can diagnostic reasoning improve:

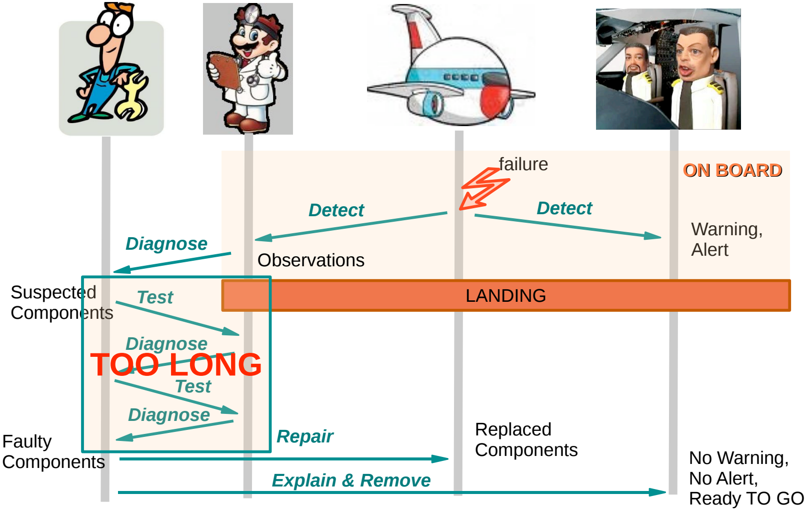
- maintenance?
- autonomy?

Diagnosis and Maintenance

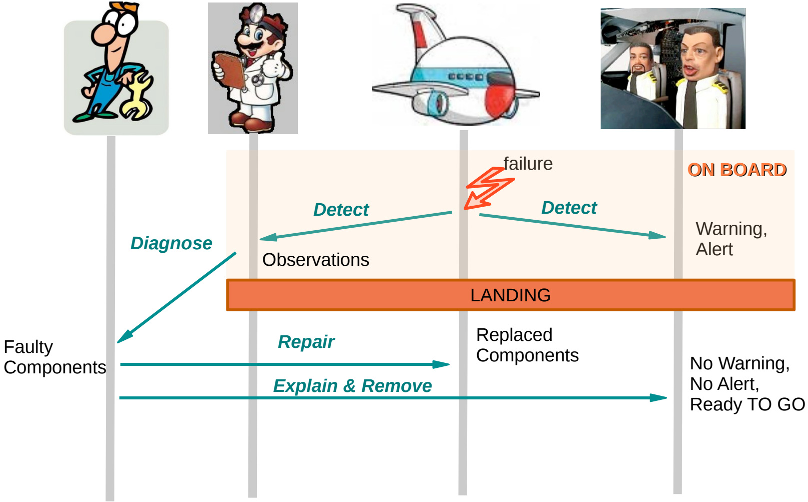
Maintenance of an embedded system: aircraft (ARCHISTIC)



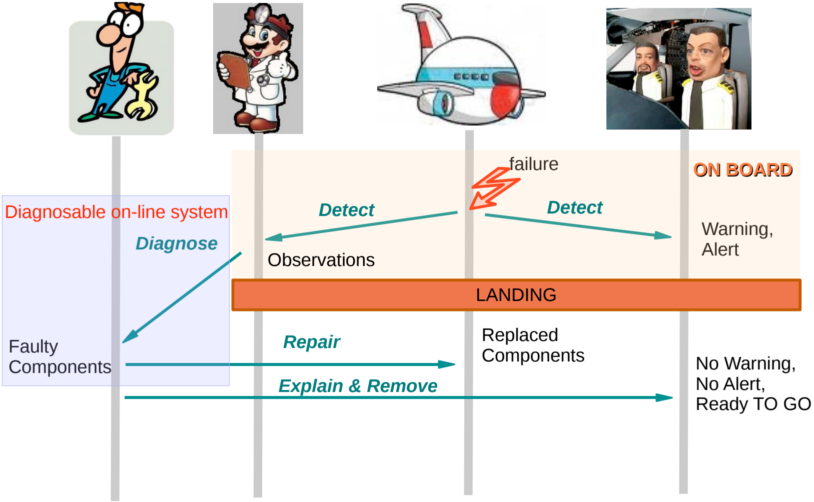
Maintenance of an embedded system: aircraft (ARCHISTIC)



Maintenance of an embedded system: aircraft (ARCHISTIC)



Ideal maintenance process implies Diagnosability

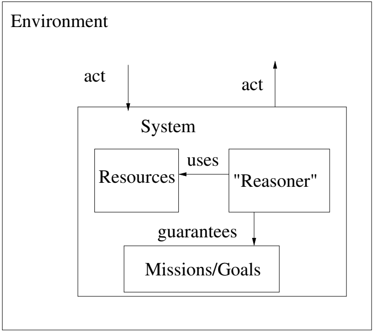


Maintenance: contributions and challenges

- Design of a diagnosis architecture that takes into account the component-based nature of the system
  - Set of communicating diagnoser agents
  - Determining for each agent, what are the components that are sufficient to monitor
    - Notion of accurate diagnosers to minimize the implementation complexity
  - Local diagnosability improves diagnosis complexity
  - Design recommendation for sensor placement to improve diagnosability
- Coupling diagnosis and prognosis to improve predictive maintenance
  - The less ambiguous the diagnosis is, the more precise the prognosis is
  - Towards a unique characterisation of the diagnosis/prognosis process.

Diagnosis and Autonomy

Autonomy of an embedded system



Benefiting of action capabilities

- Acting on its environment
  - moving around, taking objects, communicating
- Acting on itself
  - reconfiguring itself
- Decision making
  - given the current heath state, given the current environmental state, how to perform and achieve the mission?

Active diagnosis: a way to improve autonomy

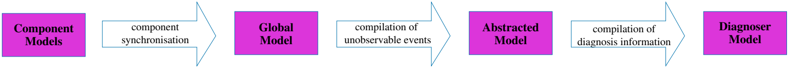
- Active diagnosis: performing actions to prune diagnostic candidates at a given time
- Two diagnostic candidates may not correspond to one unique action mode
  - Due to the ambiguity, it may be impossible to reach the mission goal with the precomputed plan.
  - Active diagnosis session: planning for ambiguity pruning
- Challenges:
  - taking into account the action capabilities at design time to analyse diagnosability
  - notion of active diagnosability
  - design recommendation for active diagnosability

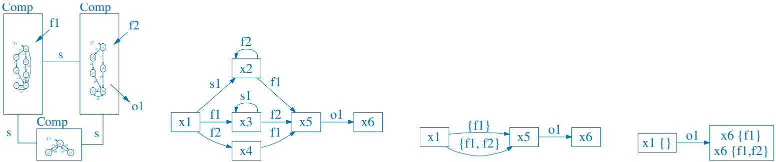
Towards self-healing systems

- Given the observability of the system (internal sensors)
- Given the repair capabilities (reconfigurations, equipement redundancies,...)
- Formal analysis to determine whether the system can heal itself
  - Self-healability: formal property
  - Capability to observe itself, diagnose and repair faults
  - Extended version of the classical diagnosability property

Embedded systems: algorithmic issues

Spectrum algorithms based on precompiled models





Let n the number of components, let F the number of faults.

Complexity: $2^{2^n \times F}$

Tradeoff between temporal and space complexity

Symbolic Finite State Machine based on BDDs

- FSM encoding into logical formulas to empirically decrease the complexity (cache)
- A state $x \in X$ is encoded with a set of $\lceil log_2(|X|) \rceil$ boolean variables:

$$x_0 = \neg b_2^X \wedge \neg b_1^X, x_1 = \neg b_2^X \wedge b_1^X, \ldots, x_3 = b_2^X \wedge b_1^X$$

- An event of Σ is encoded with a set of $\lceil log_2(|\Sigma|) \rceil$ boolean variables

$$o_1 = \neg b_2^O \wedge b_1^O \ldots$$

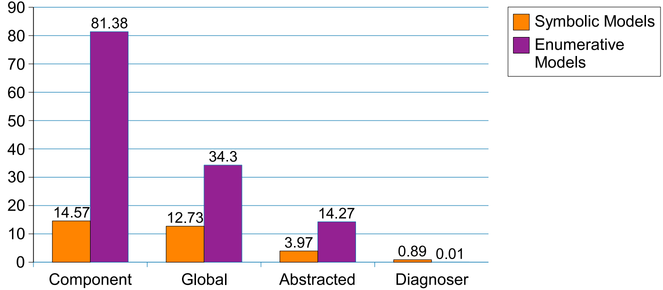
- A transition $x_{src} \xrightarrow{t} x_{trg}$ is encoded with 2 sets of $\lceil log_2(|X|) \rceil$ boolean variables for the source and target states, and a set of $\lceil log_2(|\Sigma|) \rceil$ boolean variables for the event:

$$x_1 \xrightarrow{o_1} x_2 \equiv \neg b_2^X \wedge b_1^X \wedge \neg b_2^O \wedge b_1^O \wedge b_2^{X'} \wedge \neg b_1^{X'}$$

Spectrum: Symbolic vs Enumerative

100 random scenarios containing 10000 observations each

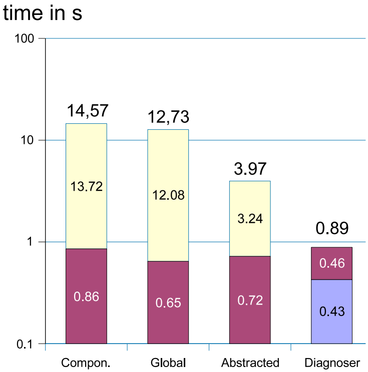
time in s



	Component	Global	Abstracted	Diagnoser
State Nr.	Ø 17.67	1063	965	18474
Trans. Nr.	Ø 34	2912	48968	120698
symb. Size (MB)	0.01	0.2	0.6	7.5
enum. Size (MB)	0.01	0.2	2.7	123.9

Spectrum: behaviour of the symbolic spectrum

100 random scenarios containing 10000 observations each



Precomputations consisting of:

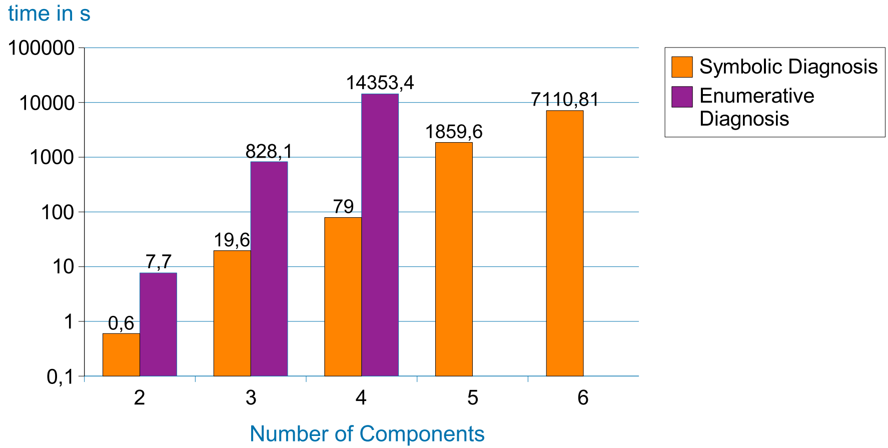
- Synchronization
- Abstraction of shared events
- Update of failure labels

Triggering observable transition

Retrieval of Diagnosis Information

Scalability of the component-based algorithm

100 random scenarios containing 10000 observations each



Taking care of the concurrency by using of Petri Nets

- Taking benefit of the compactness of Petri Nets to generate a diagnoser
- Challenge: generation of a diagnoser exponentionnally smaller than its corresponding marking graph
- Integrating symbolic time to increase expressivity (Time Petri net and chronicles)
- Taking benefit of symbolic techniques to generate marking graph efficiently (as in Tina, Romeo)

Conclusions and perspectives

- The key point is to design the diagnostic process at the same time than the design of the system itself
  - Modular diagnostic process (component-based software)
  - Formal analysis of the diagnostic objective (maintenance, autonomy, self-healing...)
  - Formal analysis of diagnosability, diagnoser accuracy, diagnosis complexity.
  - Optimizing the tradeoff between the diagnostic objective and the available computational ressources
  - Better being correct and ambiguous than incorrect
- Model-based diagnosis: relying on a complete and correct knowledge: white-box
  - We need to remove this hypothesis: grey box
  - Knowledge discovery, evolutive models, machine learning
  - How to deal with “unknown unknowns”?