LAAS-CNRS

Diagnostic causal basé cohérence pour les systèmes hybrides

R. Pons, A. Subias, L.Travé-Massuyès

Collaboration avec ACTIA Automotive
J. Thomas et H. Poulard

Journée GT S3 - 3 novembre 2011

- Diagnostic des systèmes hybrides
- Cible privilégiée : systèmes embarqués - automobile
  - Exhaustivité des modèles de fautes impossible
- Diagnostic en garage
  - Proposer la meilleure mesure au garagiste pour établir un diagnostic
  - Collaboration avec ACTIA Automotive (J. Thomas et H. Poulard)
  - PROJET AMIC-TCP Architecture Multiplexage Informatique Communication pour les Transports en Commun de Personnes (OSEO-ISI 2009-2011)

➔ Approche : basée cohérence (Modèle de comportement normal) + raisonnement abductif

➔ Approche mixant diagnostic des SED et Diagnostic SC
  - DX: Approche Diagnostiqueur
  - FDI: Graphes Causaux

Diagnostic causal basé cohérence pour les Syst. hybrides

- Modélisation du système hybride
  - Modèles Causaux des modes
- Abstraction du comportement hybride en système discret
- Construction d'un diagnostiqueur
- Raisonnement de diagnostic itératif
  - En fonction du vecteur d'observation
  - Proposition nouvelle observation discriminante

Modélisation Hybride du système: Automate Hybride

- $\Gamma = (U, Q, \Sigma, T, C, (q0,v0))$
- U l'ensemble des variables continues
- Q l'ensemble des états. Chaque état $q \in Q$ représente un mode de comportement **du système**. Q comprend les modes normaux et certains modes de fautes anticipés
- Σ fini des événements associés à l'activation des gardes (conditions booléenes dépendant de variables continues et/ou discrètes)
- $T \subseteq Q \times \Sigma \rightarrow Q$ fonction de transition
- $CSD \supseteq CSD_i$ Causal System Description : représentation des contraintes liées aux dynamiques continues du système hybride. CSD est un graphe causal défini par un ensemble d'influences liant les variables continues + un ensemble de composants associés à ces contraintes
- $(v_0,q_0) \in U \times Q$ conditions initiales du système hybride

Abstraction du comportement hybride en un système discret

- **Abstraction du domaine des valeurs des variables continues** vers ensemble fini de valeurs qualitatives
  - Fonction d'abstraction : $f_{D(vi)->\bar{D}(vi)}$:
- Association d'une **signature qualitative** Sig(q) à chaque mode
  - Capture les valeurs attendues des variables continues dans les différents modes
  - Caractérise un mode : $Sig(q) = [v_{OBS}]_q$
  - Pour chaque mode la signature est unique (choix des fonctions d'abstractions)

Abstraction du comportement hybride en un système discret

- **Abstraction des dynamiques continues** implicitement reliées aux changements de signatures en termes d'événements
- Définition d'une fonction d'abstraction qui associe un **événement induit** à chaque changement de signature

$$f_{Sig \to \sigma} : Q \times T(Q, \Sigma) \longrightarrow \Sigma^{Sig}$$

$$(q_i, q_j) \longmapsto \begin{cases} r^{o}_{i,j} \in \Sigma^{Sig}_{o} \text{ if } Sig(q_i) \neq Sig(q_j) \\ r^{uo}_{i,j} \in \Sigma^{Sig}_{uo} \text{ if } Sig(q_i) = Sig(q_j) \end{cases}$$

- Si l'ensemble d'observation est incomplet : événements induits sont tous inobservables (signature partielle)

Abstraction du comportement hybride en un système discret

- Définition de l'automate de comportement (générateur du langage hybride) $B_A(\Gamma) = (Q_{beh}, \mathbf{\Sigma}_{\mathbf{hyb}}, \mathbf{T}_{\mathbf{beh}}, q_0)$
  - Alphabet : $\mathbf{\Sigma}_{\mathbf{hyb}}$ événements discrets naturels + événements induits
  - Etats : $\mathbf{Q}_{\mathbf{beh}}$ ensemble **d'états discrets** (Q) + ensemble d'**états transitoires ($\mathbf{Q_t}$)** qui modélisent la réaction de la dynamique continue aux changements de modes
  - **Fonction de transition** : $\mathbf{T}_{\mathbf{beh}}$ décomposée en deux fonctions de transitions :

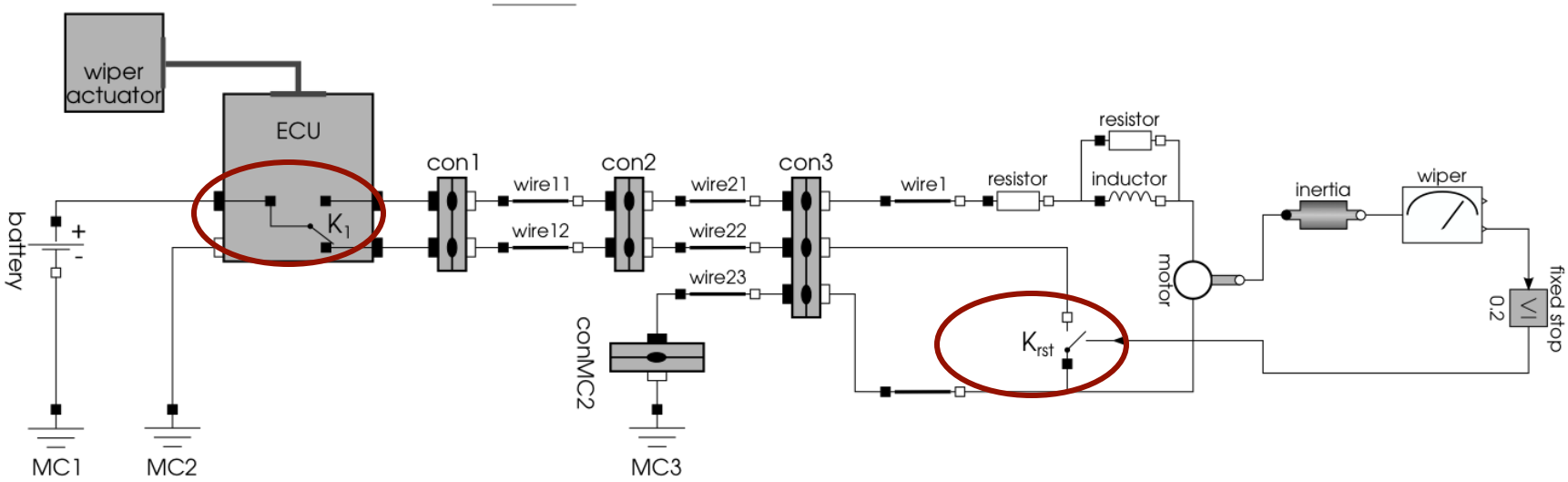
$$f_t : T \longrightarrow Q_t$$
$$t(q_i, \sigma_{i,j}, q_j) \longmapsto q_{i,j}$$

$$T_{beh} = T^1_{beh} \cup T^2_{beh}$$
$$\text{with} \begin{cases} T^1_{beh} \subseteq (Q \times \Sigma \longrightarrow Q_t) \\ T^2_{beh} \subseteq (Q_t \times \Sigma^{Sig} \longrightarrow Q) \end{cases}$$

  - Chaque transition est remplacée par deux transitions en séquence

Application au diagnostic d'une fonction embarquée

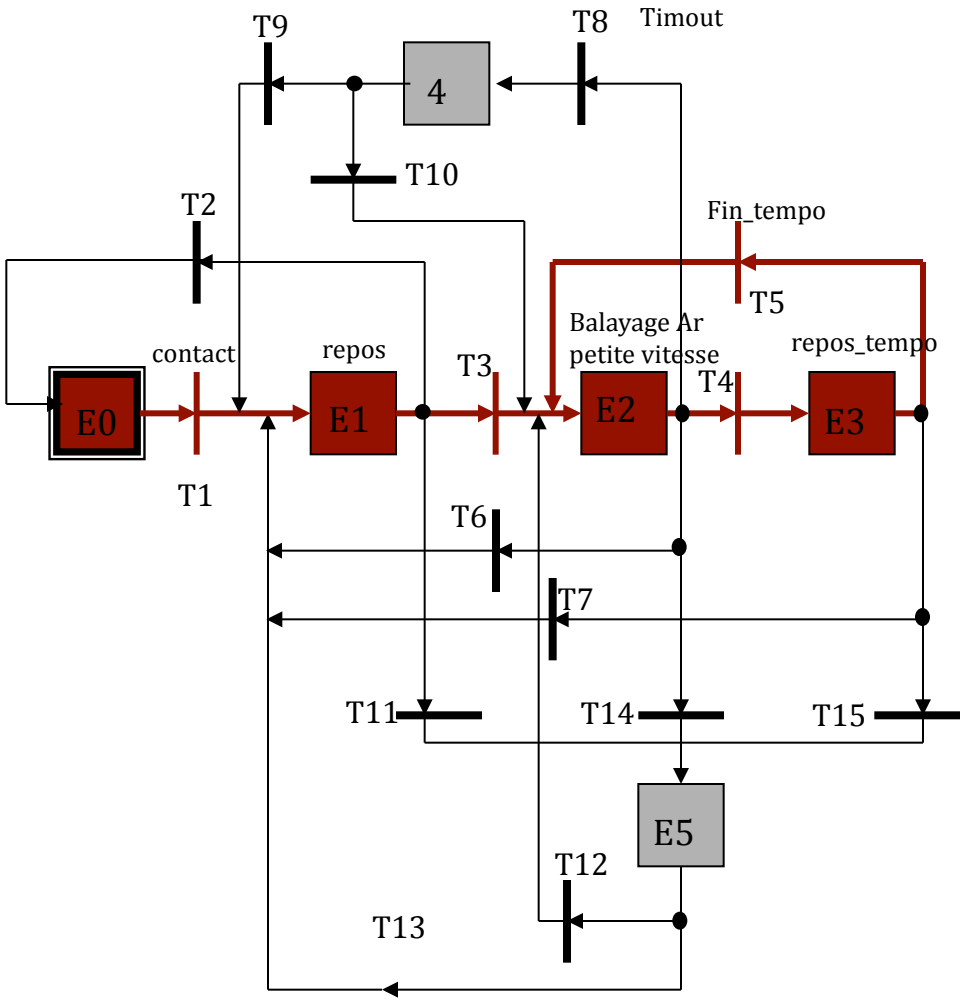
- Fonction Essuyage Vitre ARrière (EVAR) Citroën C4



2 switchs : 4 modes de comportements

Application au diagnostic d'une fonction embarquée

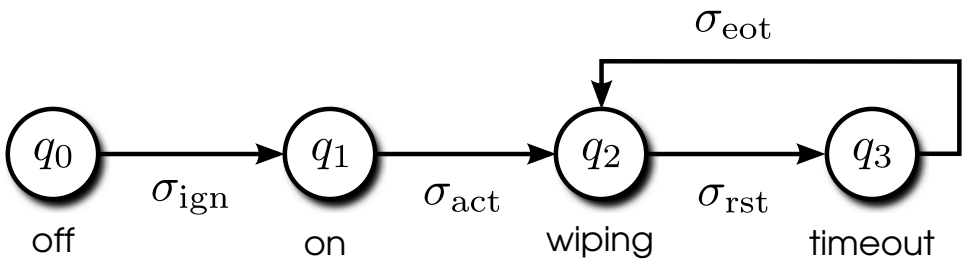
- Le modèle discret sous-jacent (issu du modèle ECU)



LAAS-CNRS

Application au diagnostic d'une fonction embarquée

Le modèle discret sous-jacent



V_1 tension d'entrée du moteur 0/12 V
V_2 tension délivrée par le capteur arrêt fixe X/0 V
Ω vitesse de rotation du balai
V_{groung}/ V_{bat} tensions masse/batterie

Variable abstraites

	q_0 Off	q_1 On	q_2 Wiping	q_3 Timeout
V_1	0	0	1	0
V_2	1	1	1	0
Ω	0	0	1	0
V_{bat}	1	1	1	1
V_{grd}	1	1	1	1

Continuous variables vs. modes

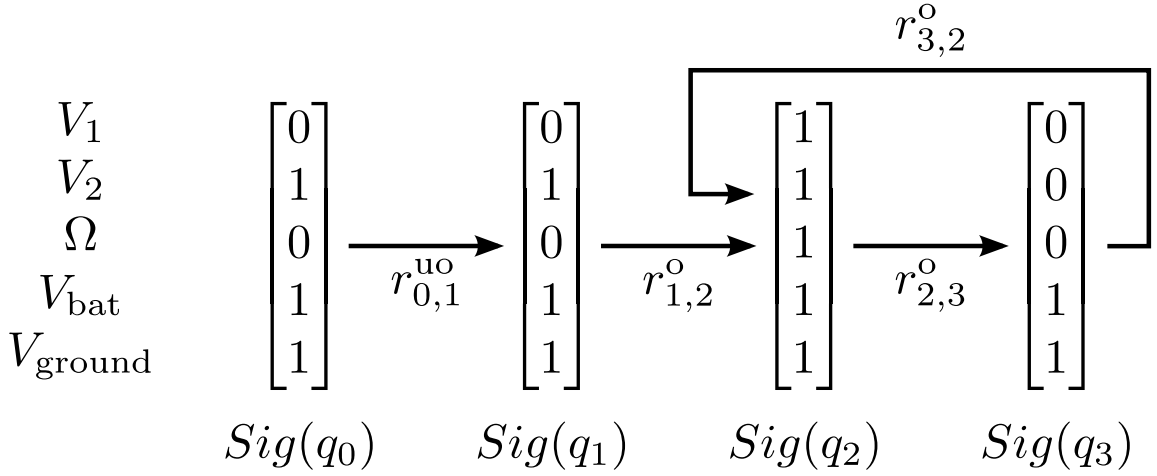
Signature qualitative
(issues de simulations Modélica)

$$q_0 \xrightarrow{\sigma_{\text{ign}}} q_1\,, \quad q_1 \xrightarrow{\sigma_{\text{act}}} q_2\,, \quad q_2 \xrightarrow{\sigma_{\text{rst}}} q_3\,, \quad q_3 \xrightarrow{\sigma_{\text{eot}}} q_2$$

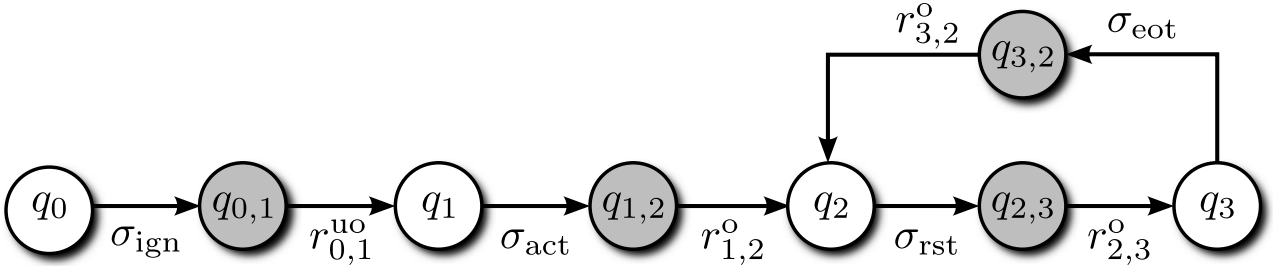
Events

Application au diagnostic d'une fonction embarquée

Le modèle abstrait discret de la dynamique continue



L'automate de comportement

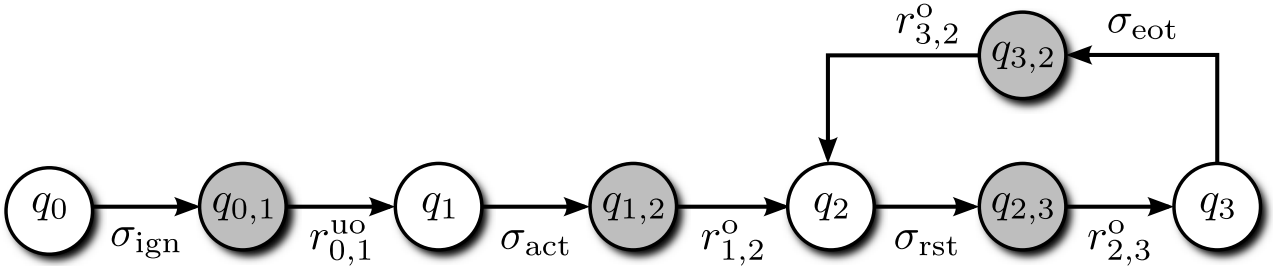


Construction d'un diagnostiqueur Partiel

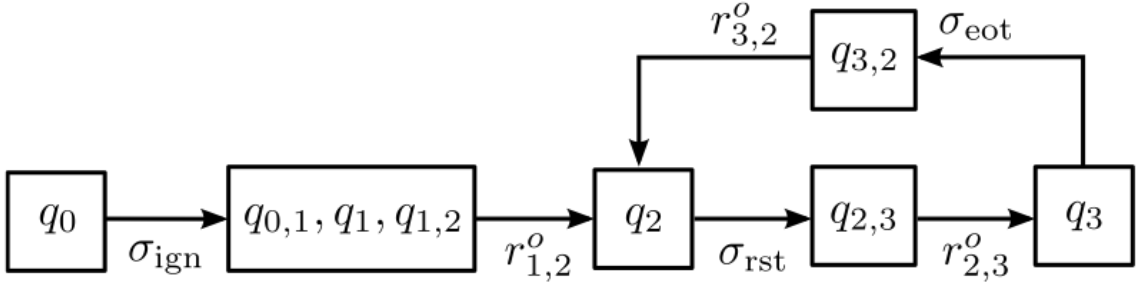
- **Extension du diagnostiqueur de Sampath** aux systèmes hybrides + comportements normaux
- **Diagnostiqueur Partiel** : pas toutes les trajectoires de fautes (certaines trajectoires de fautes + trajectoires comportement normal)
- Construit à partir de l'automate de comportement BA(Γ)
- PDiag(BA(Γ)) = (Q_{PD}, $\mathbf{\Sigma}_{PD}$, T_{PD}, q_{PD0})
  - $Q_{PD} \subseteq 2^{Q_{beh} \times \mathcal{L}}$ ensemble des états : les états sont des ensembles de couples (état de l'automate de comportement, label)
    - $q_{PD} = \{(q_1; l_1); (q_2; l_2)\ldots(q_n; l_n)\}$ avec $q_i \in Q_{beh}$ et $l \in \mathcal{L}=2^{\Sigma_{hyb\ uo}}$
  - $\mathbf{\Sigma}_{PD}=\mathbf{\Sigma}_{\mathbf{hyb}\ o}$: ensemble des événements observables
  - $T_{PD} \subseteq Q_{PD} \times \mathbf{\Sigma}_{PD} \longrightarrow Q_{PD}$: fonction de transition
  - $q_{PD0} = \{(q_0, \varnothing)\}$ état initial (supposé normal)
- Si l'ensemble d'observation est incomplet : Pdiag*(BA(Γ))

Application au diagnostic d'une fonction embarquée

L'automate de comportement



le diagnostiqueur (avec vecteur d'observation incomplet)



Raisonnement de diagnostic

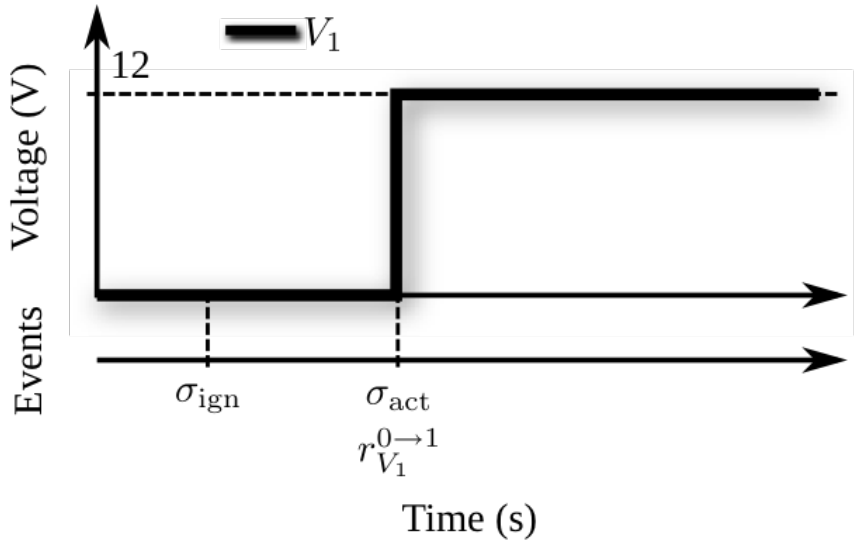
- **Approche basée cohérence** : modèles de référence
  - Diagnostiqueur Partiel + Modèles causaux
  - Observations : $s_{obs} = \{\sigma^1, \sigma^2, \ldots, \sigma^N\}$ séquence d'événements observables

- **Etape1 : Détection des fautes et génération des hypothèses** sur les modes de références
  - Synchronisation de s_{obs} avec le Diagnostiquer Partiel
  - Détection de faute si pas de synchronisation avec une trajectoire complète du Diagnostiqueur Partiel
  - Le dernier état de chaque trajectoire synchronisée donne un mode de référence possible pour expliquer l'incohérence
  - Q_{ref}=ensemble des modes de référence
  - Ensemble d'ambiguïté initialisé : $\mathcal{A}$=COMP ensemble des composants du système

Application au diagnostic d'une fonction embarquée

Scénario de faute : bobine moteur HS – commande envoyée par ECU (σ_{act}) – le balai n'atteint jamais la position de repos et l'ECU ne reçoit pas l'événement associé (σ_{rst}) – exonération de la batterie et ses connections

Mesure garagiste : V_1: tension d'alimentation moteur (vecteur d'observation incomplet)



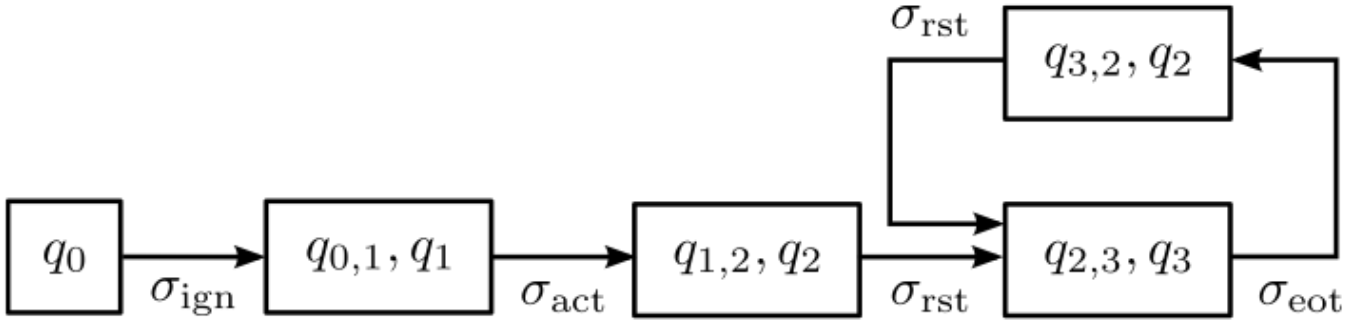
Séquence d'observation :

$s_{obs} = \{\sigma_{ign}, \sigma_{act}\}$

Application au diagnostic d'une fonction embarquée

Séquence d'observation : $s_{obs} = \{\sigma_{ign}, \sigma_{act}\}$

Diagnostiqueur Partiel : Pdiag*(BA(Γ)) (mesure que V_1 donc tous les événements induits sont inobservables)

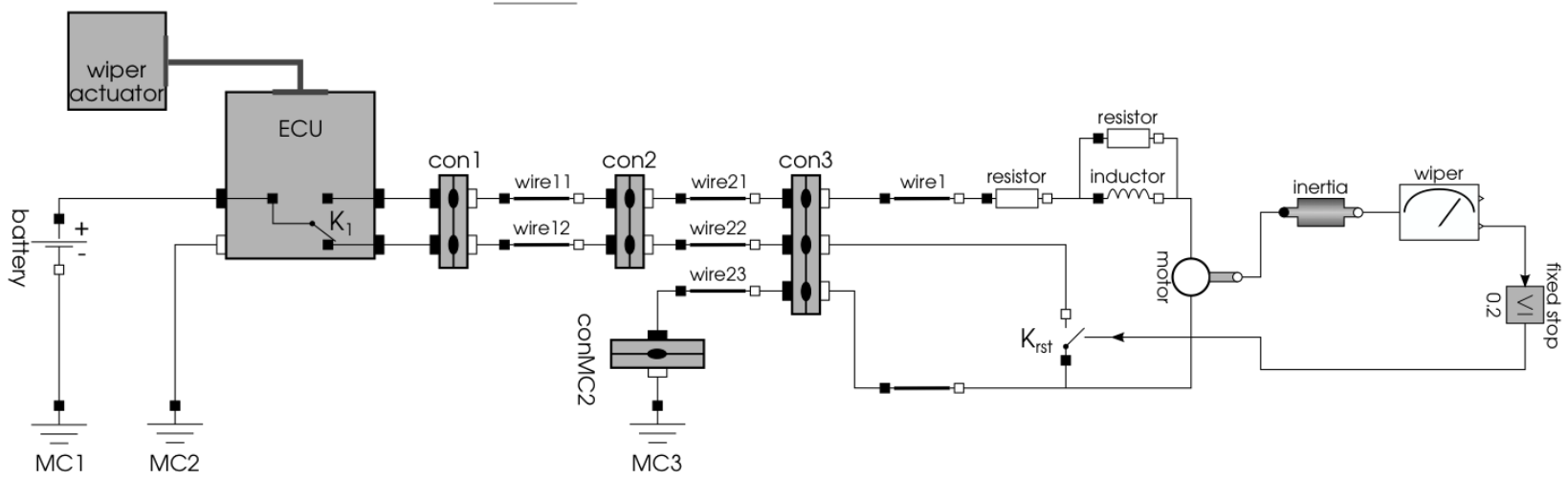


Synchronisation possible avec la sous-trajectoire $\{q_0, q_{0,1}, q_1, q_{1,2}, q_2\}$.
Trajectoire incomplète => **détection de faute**
Q_{ref} = {q1, q2}, car sémantiquement $q_{1,2}$ est équivalent à q_1 ou q_2

$\mathcal{A}$={motor, wiper, rest sensor, $K_{rst\ switch}$, $K_{1\ switch}$, wireA, wireB, wireD, wireE}

Application au diagnostic d'une fonction embarquée

- Fonction Essuyage Vitre ARrière (EVAR) Citroën C4



$\mathcal{A}$={motor, wiper, rest sensor,$K_{rst\ switch}$, $K_{1\ switch}$, wireA, wireB, wireD, wireE}

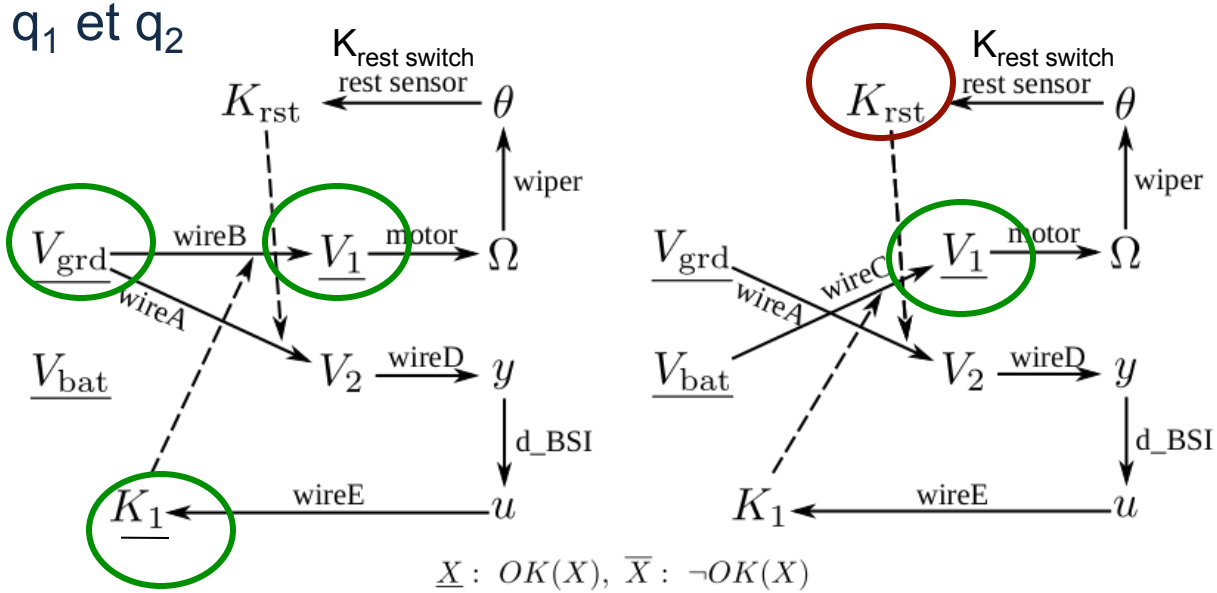
Raisonnement de diagnostic

- **Etape 2 : Génération des hypothèses de diagnostic**
  - Chaque élément (i.e. mode) de Q_{ref} peut potentiellement expliquer la faute : $\mathcal{A}$=COMP $\cap \cap_i\{\mathcal{A}_i\}$
  - **Construction d'un graphe causal CSD_i pour chaque $q_i \in Q_{ref}$**
    - Graphe orienté - Arc entre deux sommets v_i et v_j existe si la variable v_i (cause) influence le variable v_j (effet) - Variables labellisées par des Tests
  - Application du diagnostic **à base de modèle causal** pour chaque $q_i \in Q_{ref}$
    - Le graphe est parcouru vers l'arrière - une variable est qualifiée de OK si la valeur observée correspond à la valeur prédite
    - **Adaptation du diagnostic logique** (Reiter)

Definition (Diagnosis problem). It is a triple (CSD, COMP, OBS) where (CSD, COMP) is the causal system model and OBS a set of observations i.e. a tuple that qualifies every observed variable v_i as $\neg OK(v_i)$ or $OK(v_i)$.

Application au diagnostic d'une fonction embarquée

Graphes causaux q_1 et q_2



$S_{obs} = \{\sigma_{ign}, \sigma_{act}\}$ => K_1 OK en q1 et K_{rst} not OK

Signature partielle observée = Signature partielle théorique **=>V1 OK en q1 et q2**

V_1 $[0]$ (q_0) $\longrightarrow$ $[0]$ (q_1) $\longrightarrow$ $[1]$ (q_2) $\rightarrow$ ↯

$\mathcal{A}$ = {$K_{rest\ switch}$, rest sensor, wiper, motor}

Raisonnement de diagnostic

- **Etape 3 : Sélection du Test**
  - Détermination de la prochaine variable à tester pour maximiser la réduction de l'ensemble d'ambiguïté (et minimiser le cout total de test)
  - Méthode : gReedy diAgnostic Prioritization by ambiguiTy Reduction (RAPTOR)
    - Gonzalez-Sanchez et al 2011 (DX2011)
    - Distribution uniforme des fautes dans le système
    - Matrice de signature Composants/Tests S (tests couvrants/ couverture des tests)
    - Définition de groupes d'ambiguïté (composants non discriminables suite à à k tests)
    - Métrique de l'effort résiduel de diagnostic si les composants sont pris au hasard dans ces groupes d'ambiguïté g_i

$$G(AG) = \sum_{i=1}^{L} Pr(g_i) E[C_{d_i}] = \sum_{i=1}^{L} \frac{|g_i|}{|COMP|} \frac{|g_i| - 1}{2}$$

Réduction d'Ambiguïté

$$AR(\mathcal{S}, T_i) = G(AG(\mathcal{S})) - G(AG(\mathcal{S} \| T_i))$$

et retour étape 2

Application au diagnostic d'une fonction embarquée

Matrice de Signature des Tests (1 par mode)

q_1 / q_2	T_{V_1}	T_{V_2}	T_θ	T_Ω
motor	0/0	0/0	1/1	1/1
wiper	0/0	0/0	1/1	0/0
rest sensor	0/0	0/0	0/0	0/0
K_{rst} switch	0/0	0/0	0/0	0/0
K_1 switch	0/0	0/0	0/0	0/0
wireA	0/0	1/1	0/0	0/0
wireB	1/0	0/0	0/0	0/0
wireD	0/0	0/0	0/0	0/0
wireE	0/0	0/0	0/0	0/0

- Groupe d'ambiguïté g_1={$K_{\text{rst switch}}$, rest sensor, wiper, motor} (dans q_1 et q_2) and G(AG) = 6/13
-Tests T_Θ et T_Ω coupent le groupe d'ambiguïté en deux groupes
- G(AG||T_Θ)=1/13 et G(AG||T_Ω)=3/13
- Proposition du test de Θ -> $\mathcal{A}$ = {wiper, motor} (Θ=0 conflit en q_2)
- Mise à jour de la Table de signature de Test
-Proposition du test de Ω (% V_2)-> $\mathcal{A}$ = {motor}

Conclusion

- Approche de diagnostic des Systèmes hybrides
- Fondements domaine SED & SC.
- Pas de modèle de faute -> une extension des approches basées sur des dictionnaires de fautes pour prendre en compte des fautes non anticipées e.g. fautes de déviations de paramètres

Et Ensuite ?

- Prise en compte de l'hypothèse d'exonération pour les circuits dont certaines branches peuvent ne pas être alimentées dans certains modes?
- Cadre distribué w.r.t. problème d'explosion combinatoire

Quelques références

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., and Teneketzis, D. (1995). Disgnosability of discrete-event systems. IEEE Transactions on Automatic Control, 40(9), 1555-1575.

Gonzalez-Sanchez, A., Abreu, R., Gross, H., and Gemund, A.V. (2011). Raptor: Greedy diagnostic prioritization by ambiguity group reduction. In Proceedings of the 22nd International Workshop on Principles of Diagnosis, DX2011, 84-91

Reiter, R. (1987). A theory of diagnosis from first principles. Articial Intelligence, 32(1), 57-95

Bayoudh, M., Trave-Massuyes, L., and Olive, X. (2008b) Hybrid systems diagnosis by coupling continuous and discrete event techniques. Proceedings of the IFAC World Congress Seoul Korea, 7265-7270

LAAS-CNRS

Diagnostic causal basé cohérence pour les systèmes hybrides

R. Pons, A. Subias, L.Travé-Massuyès

Collaboration avec ACTIA Automotive
J. Thomas et H. Poulard

Journée GT S3 - 3 novembre 2011