Contrôle des SED avec urgence, évitabilité et inéluctabilité

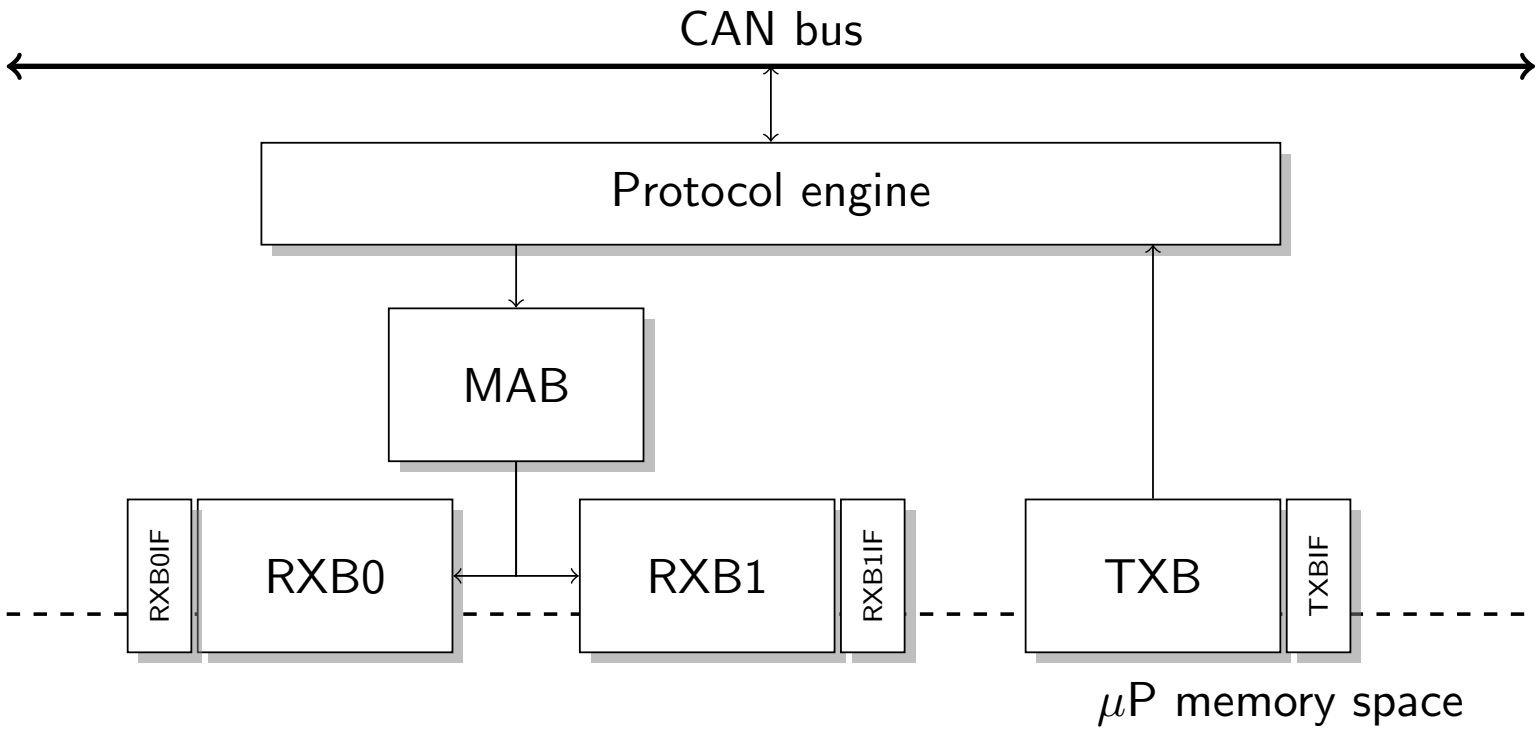
MSR 2019

Angers - 13-15 novembre, 2019

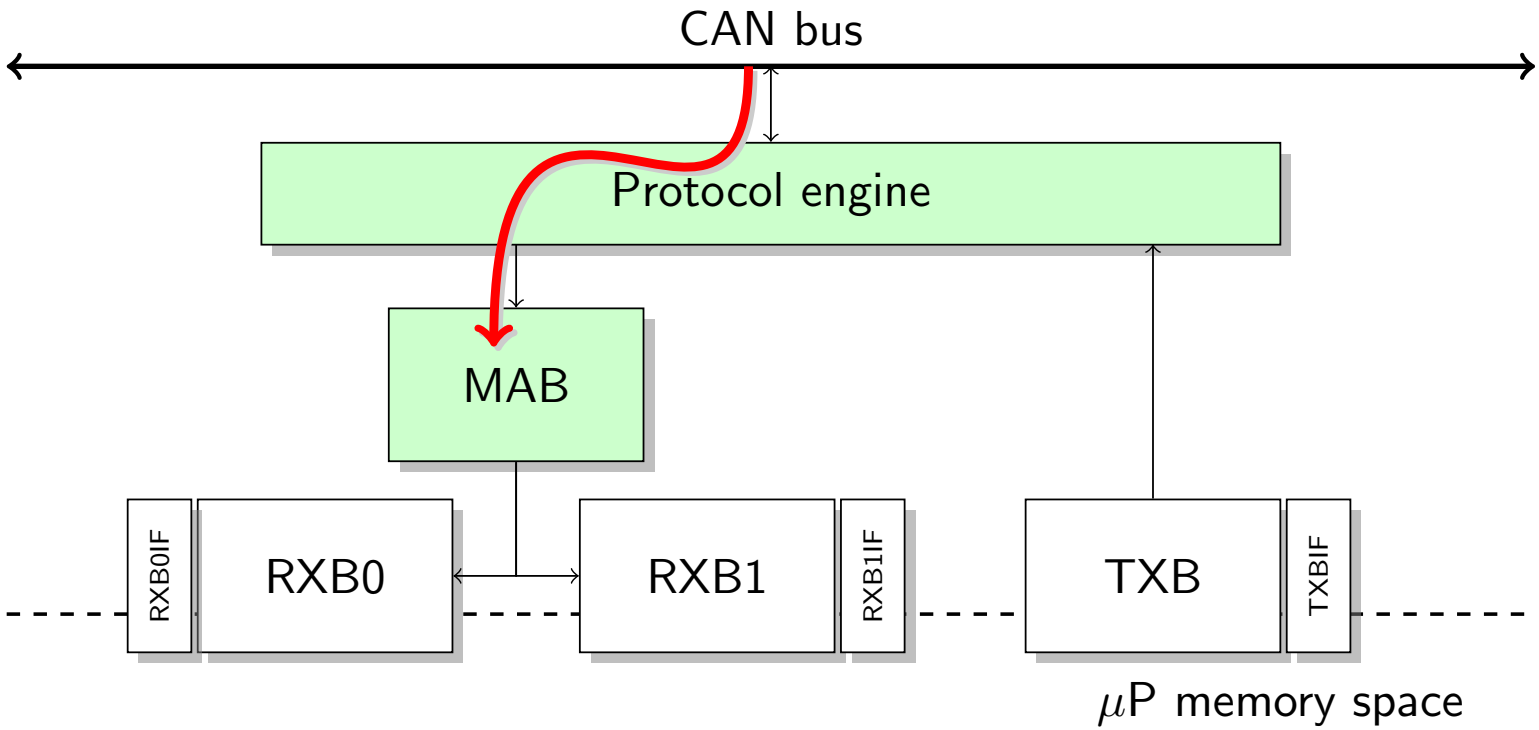
Jean-Luc Béchennec, Didier Lime, Olivier H. Roux

Outline

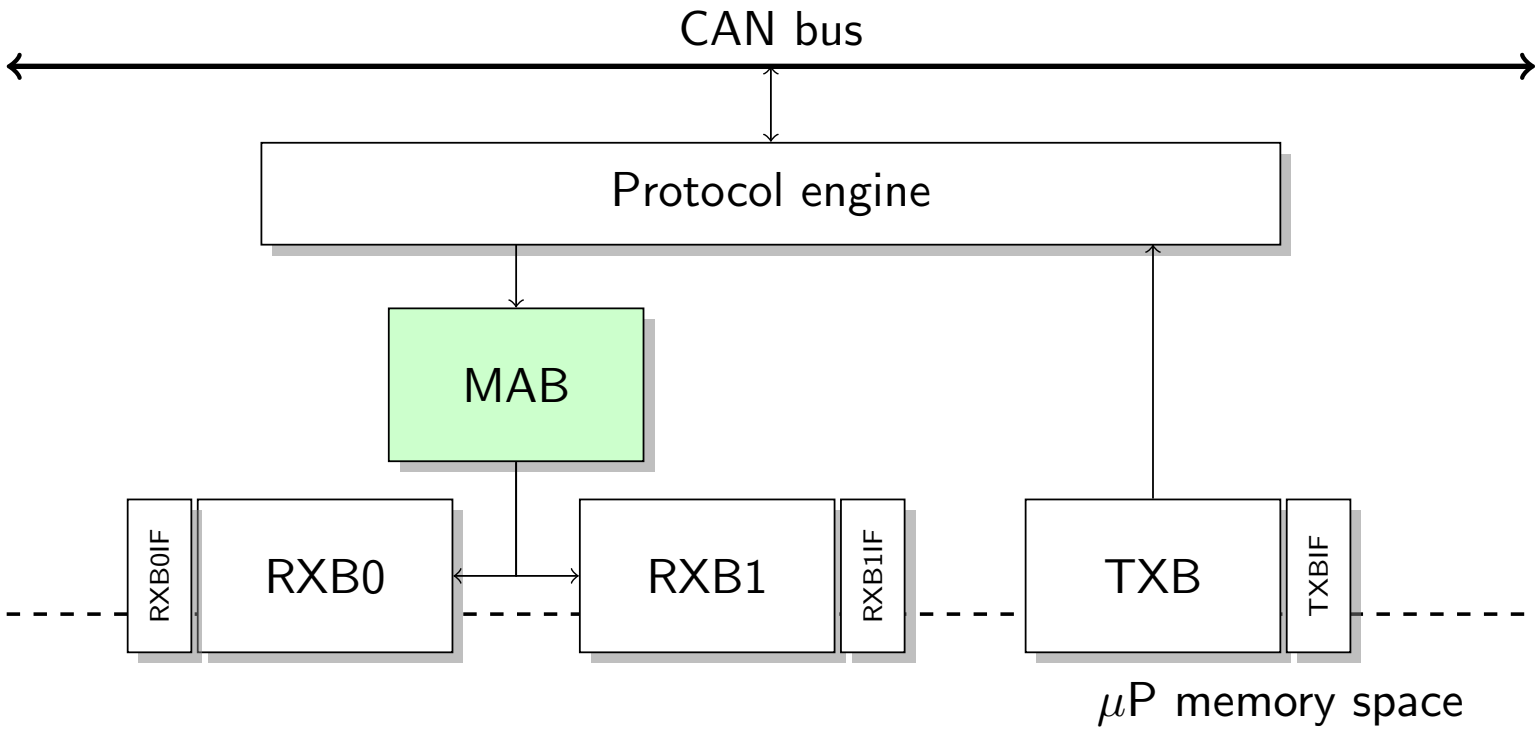
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

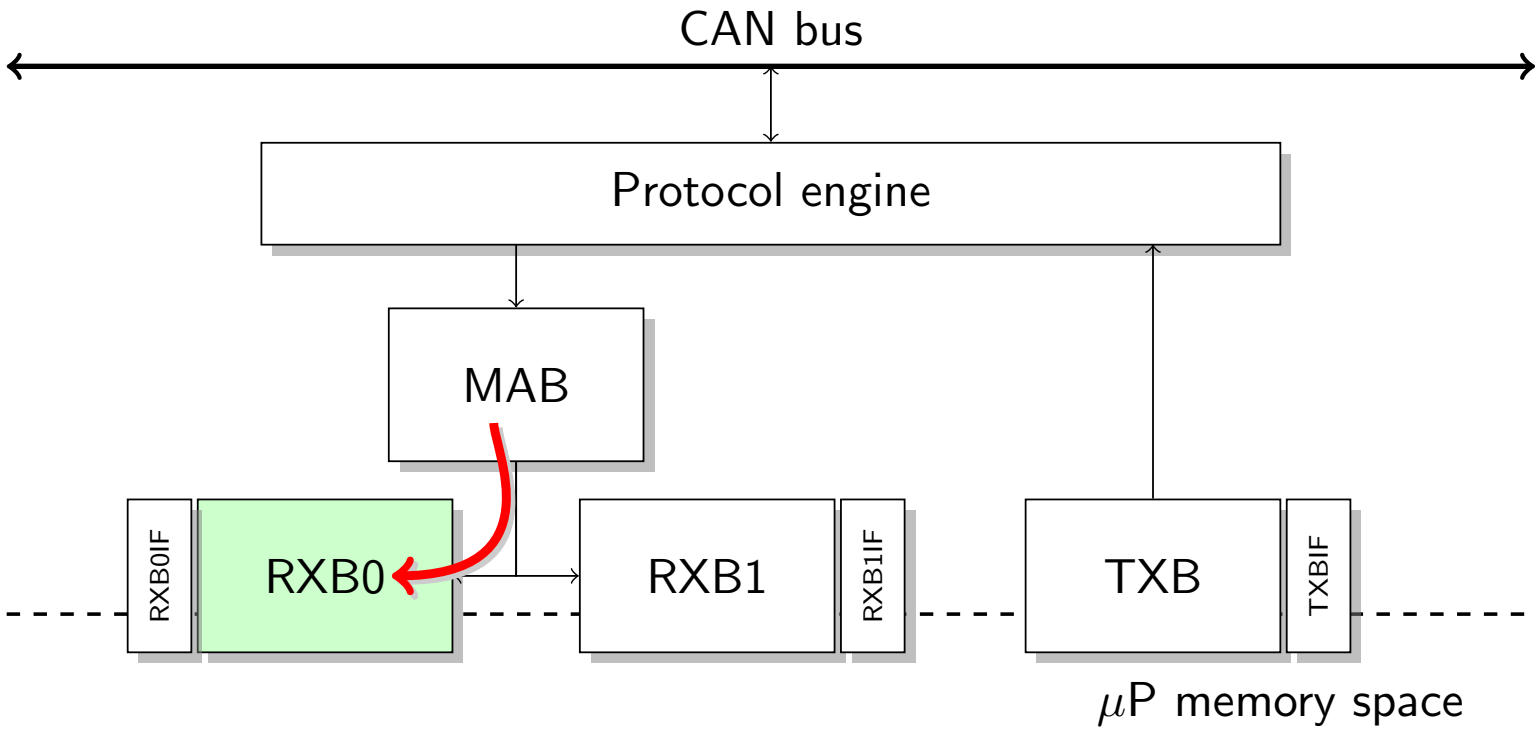
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

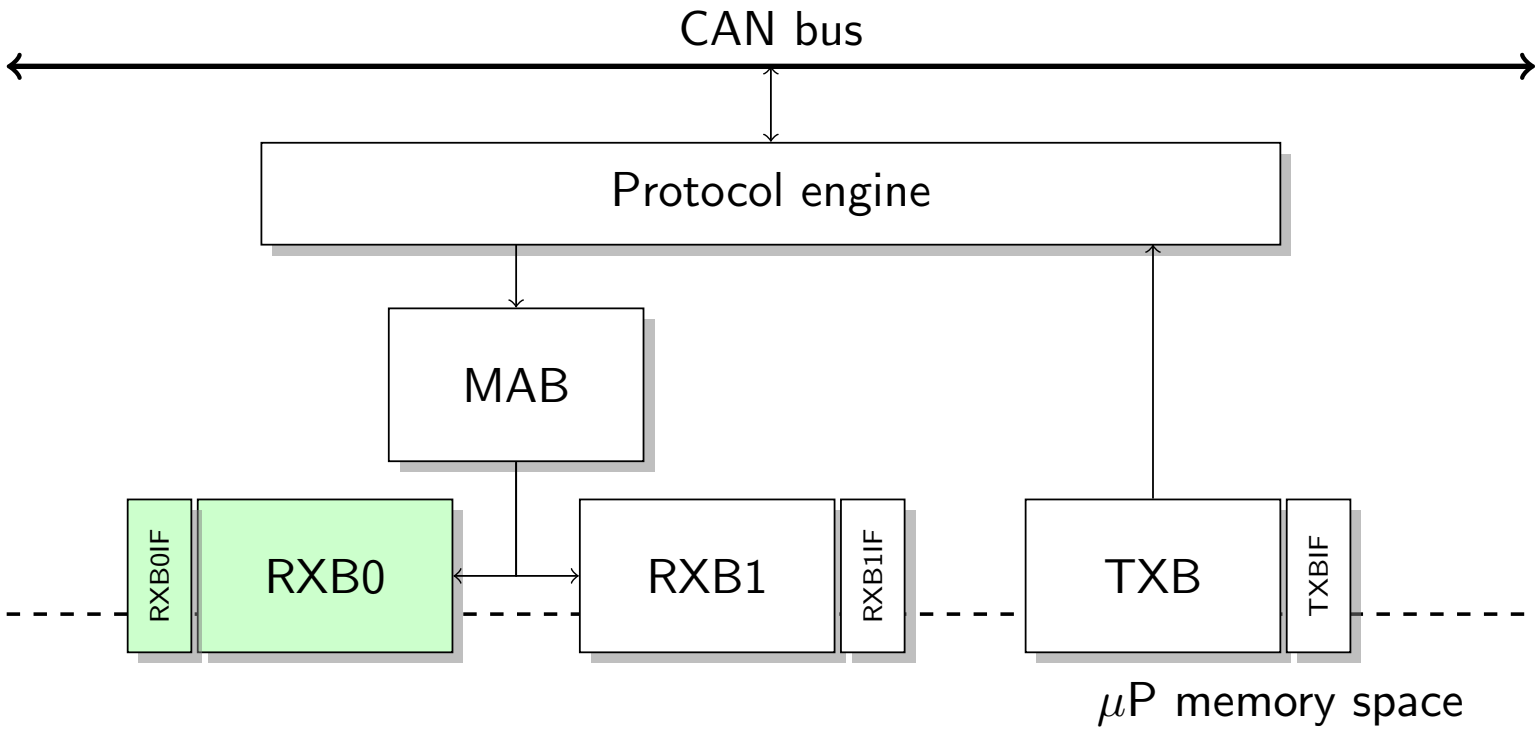
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

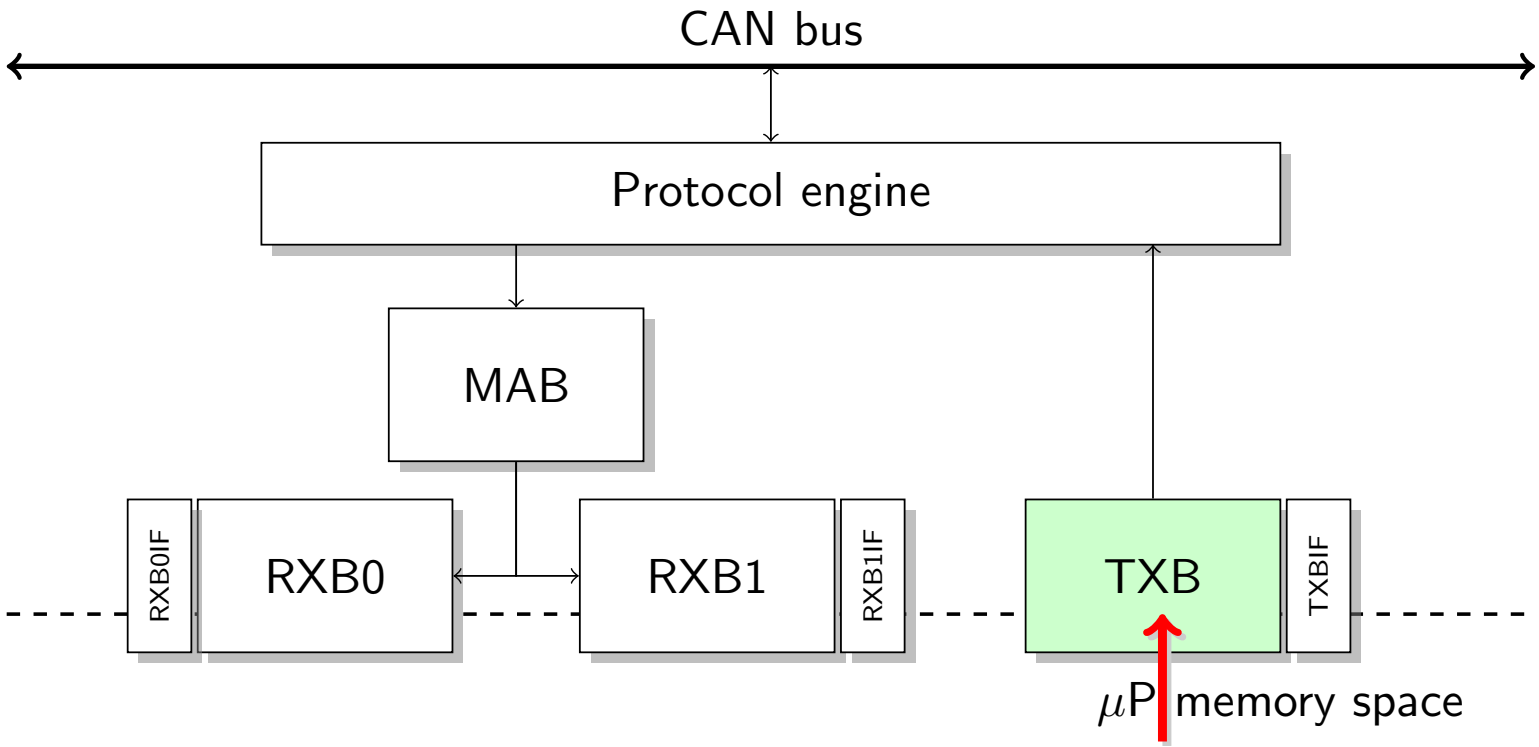
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

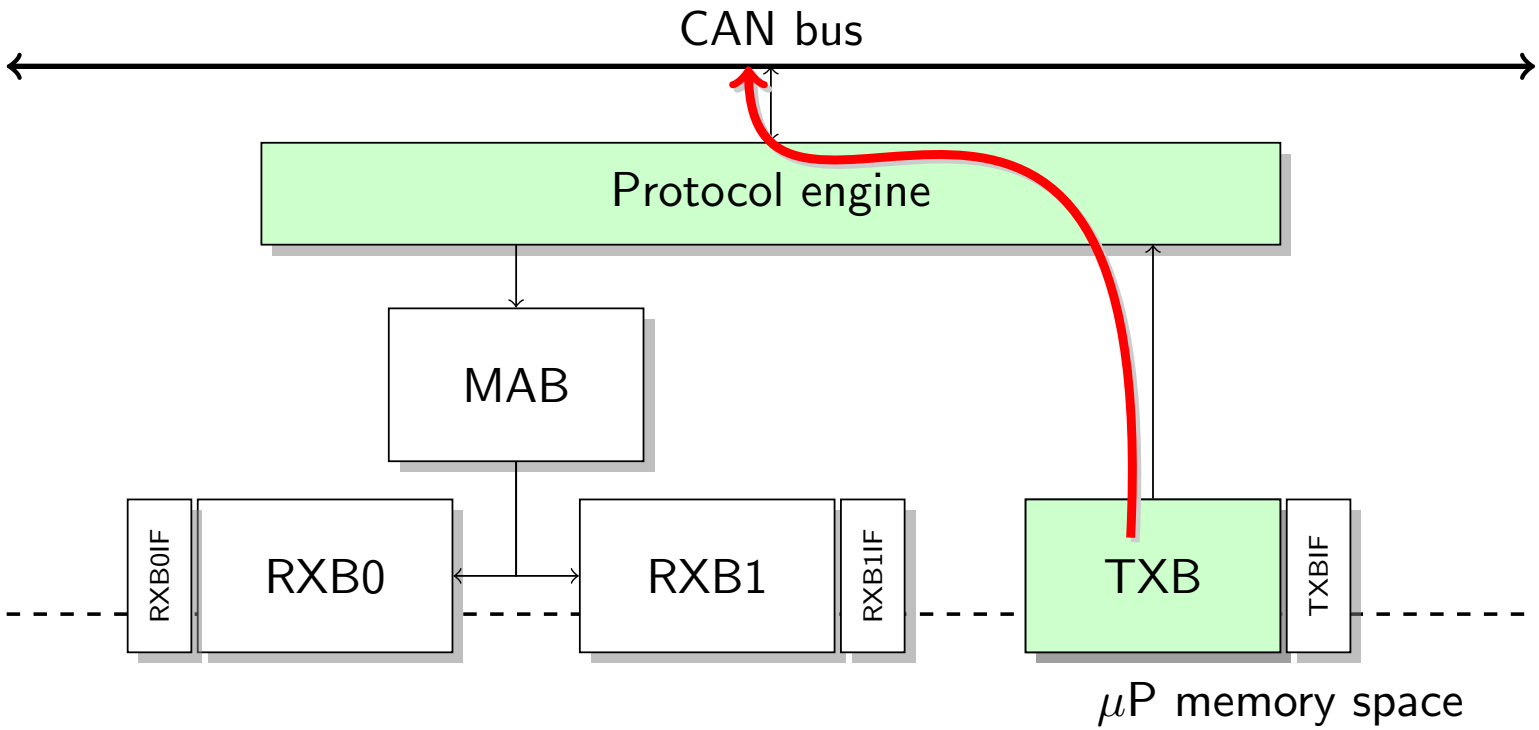
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

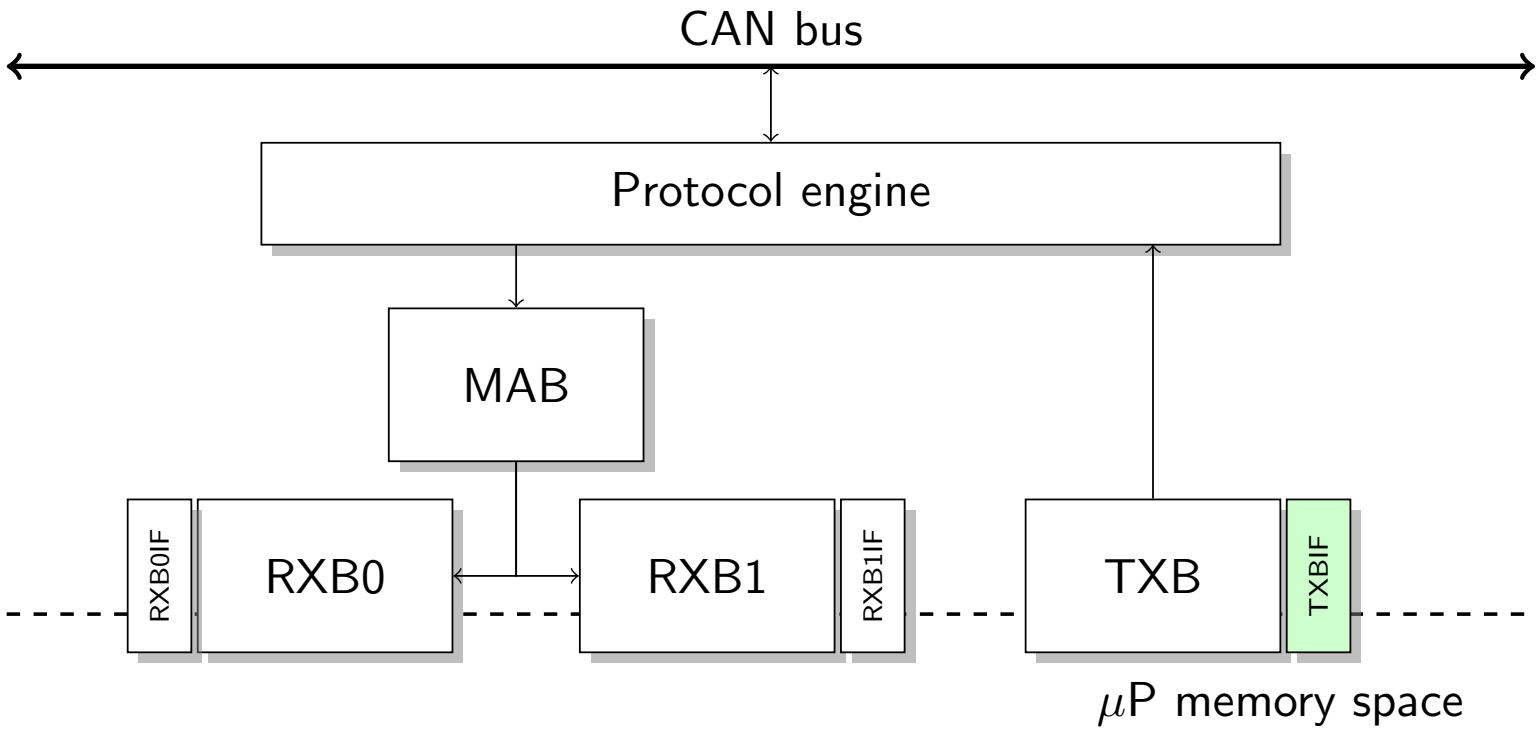
CAN device


CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

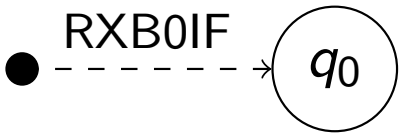
CAN device

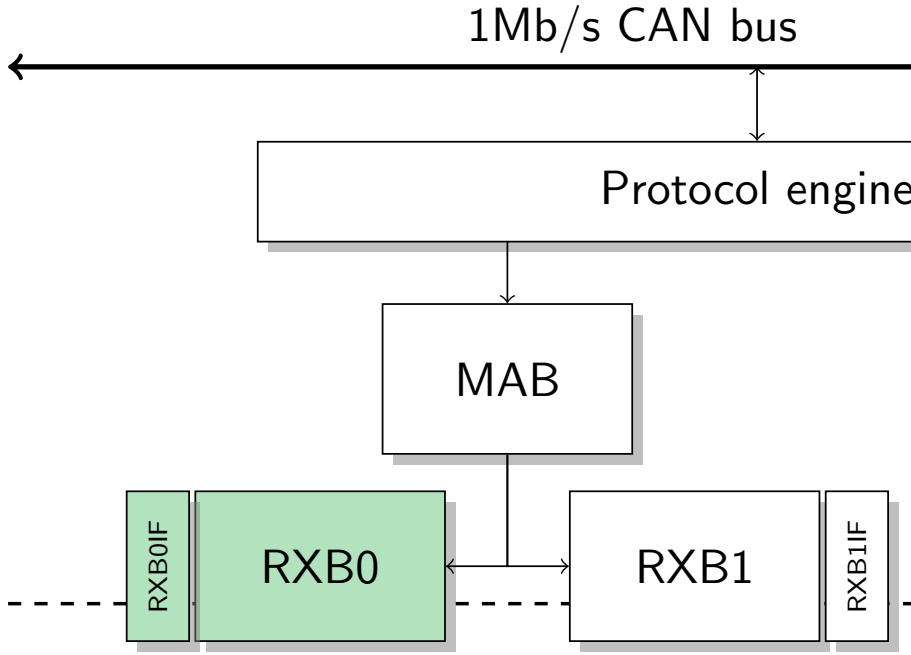

CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

CAN device

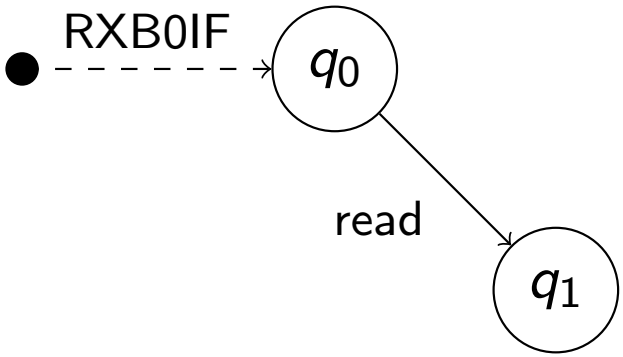

CAN bus
Protocol engine
MAB
RXB0IF
RXB0
RXB1
RXB1IF
TXB
TXBIF
μP memory space

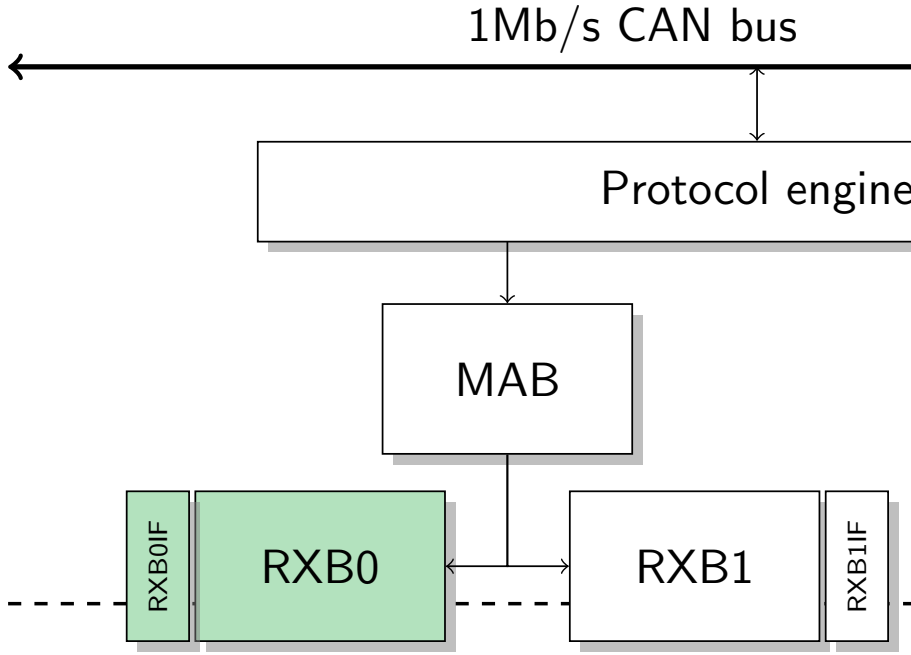
Application to device drivers : avoidable actions



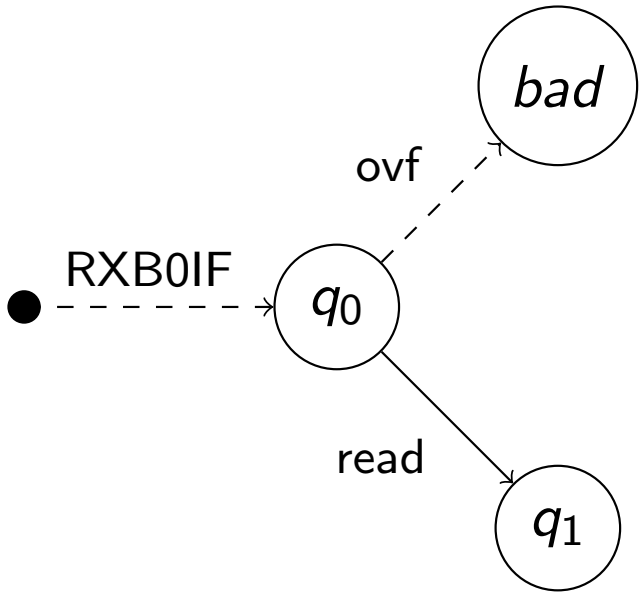


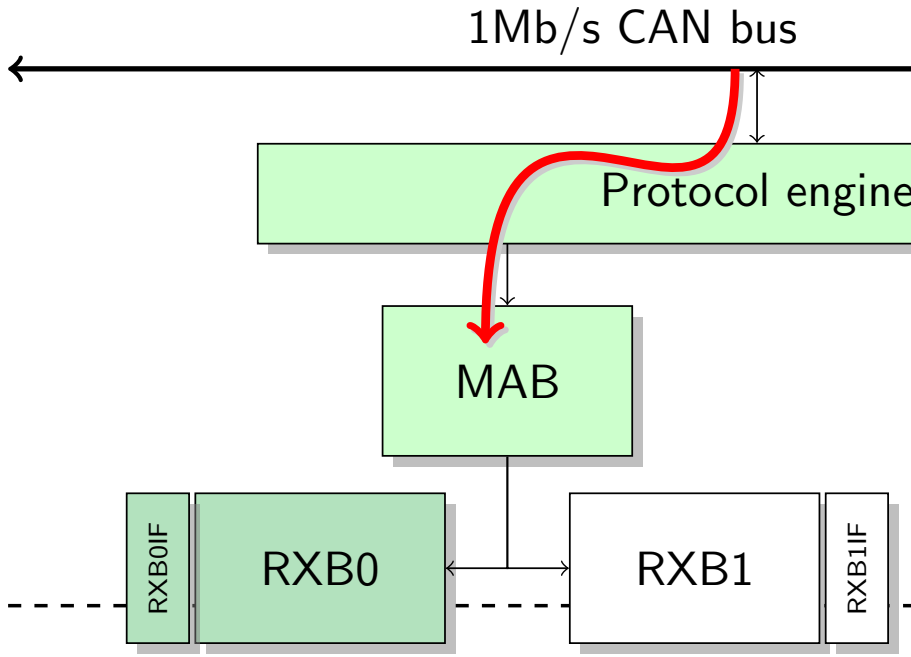
Application to device drivers : avoidable actions



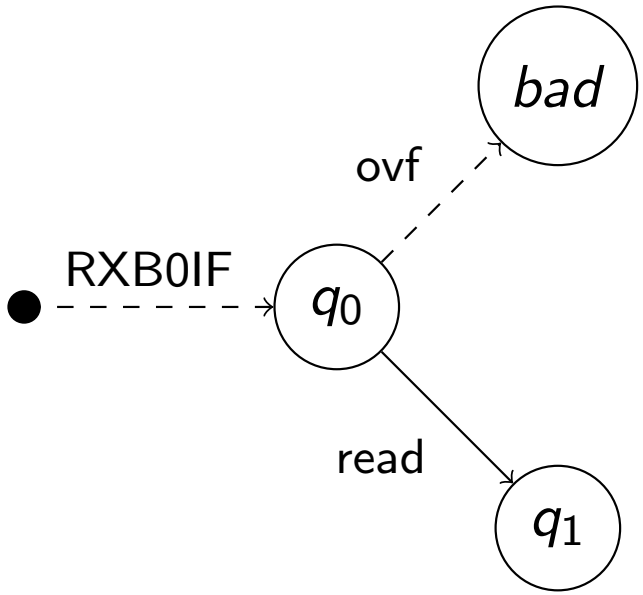


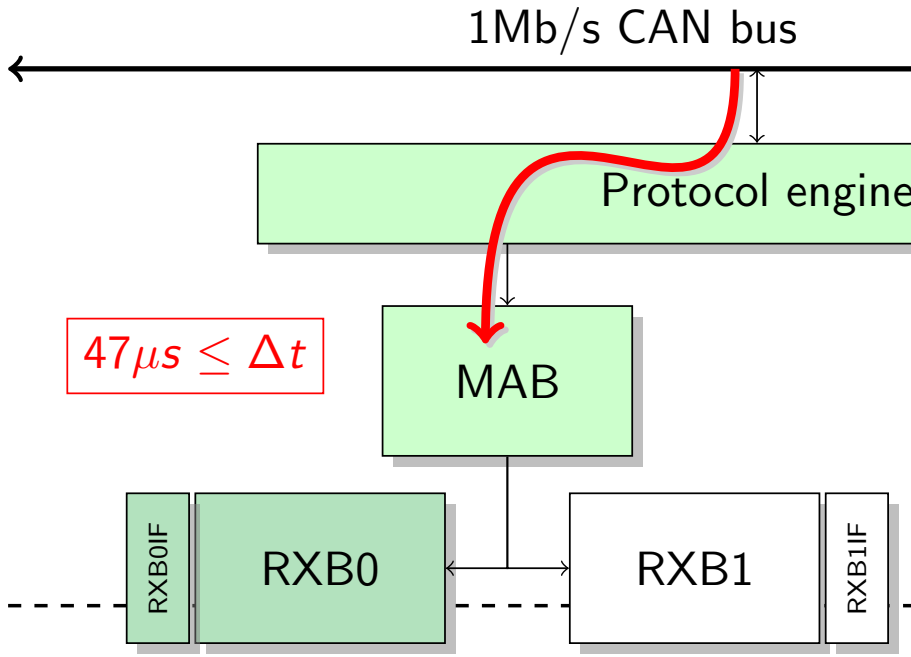
Application to device drivers : avoidable actions



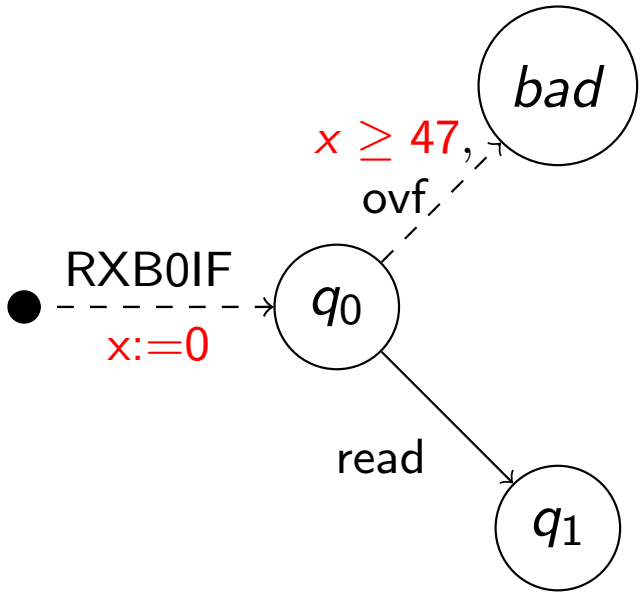


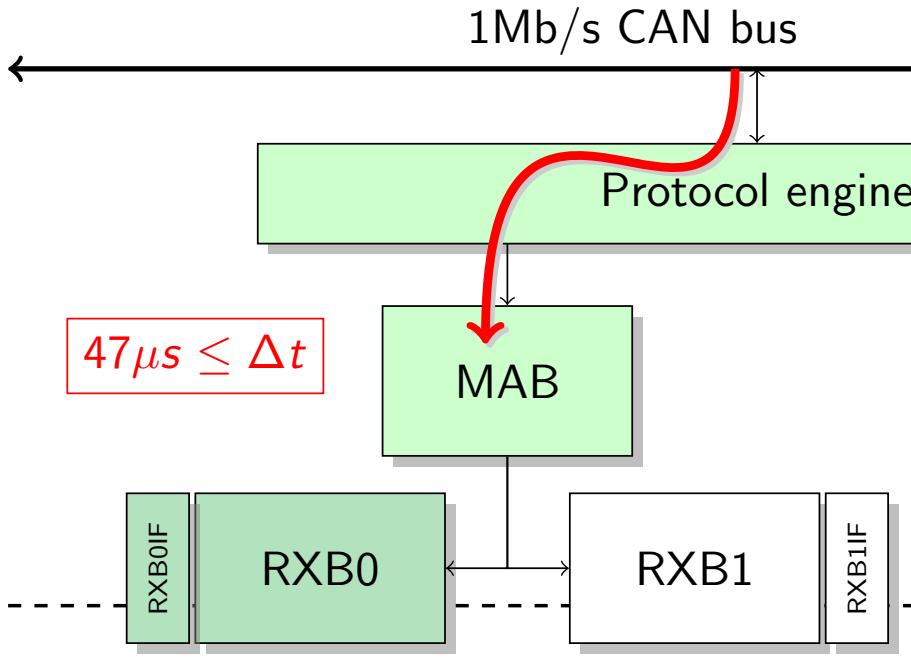
Application to device drivers : avoidable actions



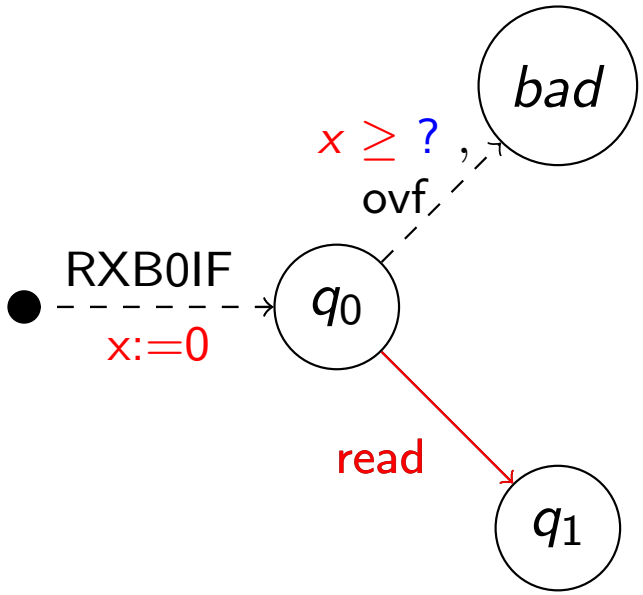


Application to device drivers : avoidable actions

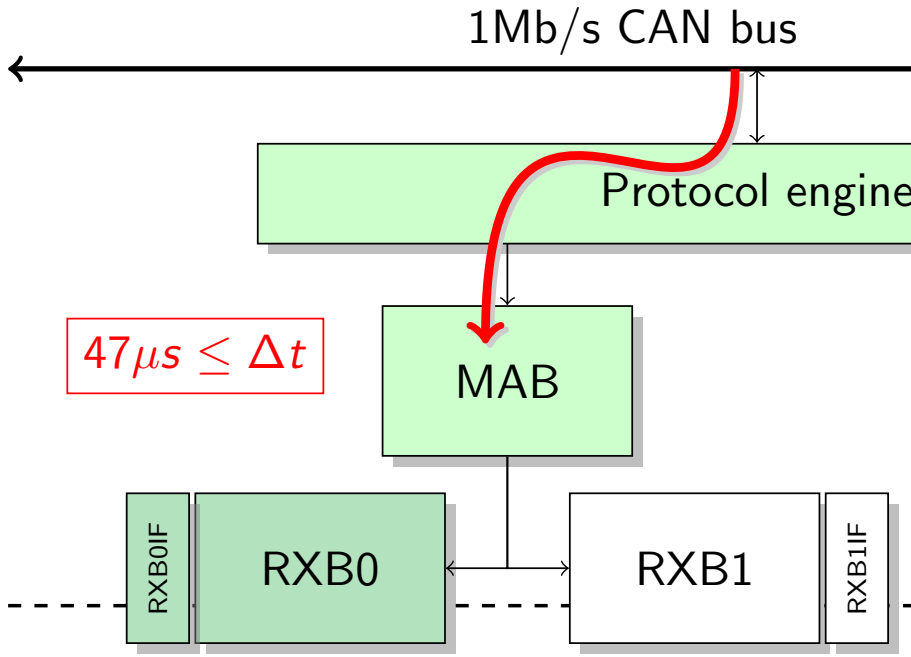




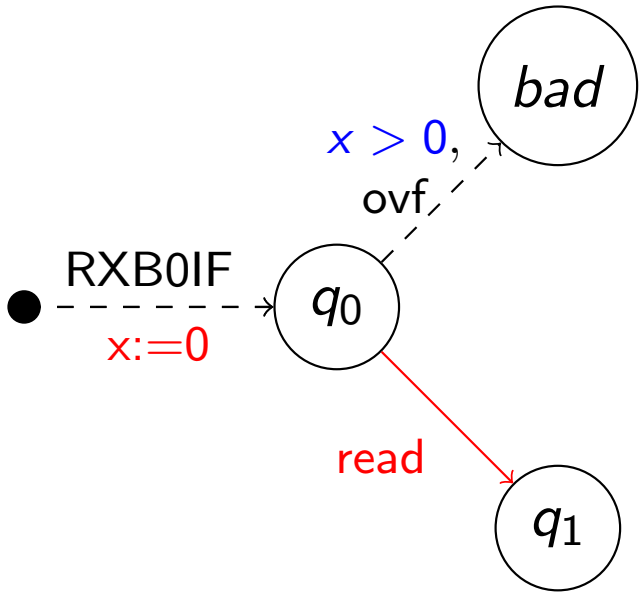
Application to device drivers : avoidable actions



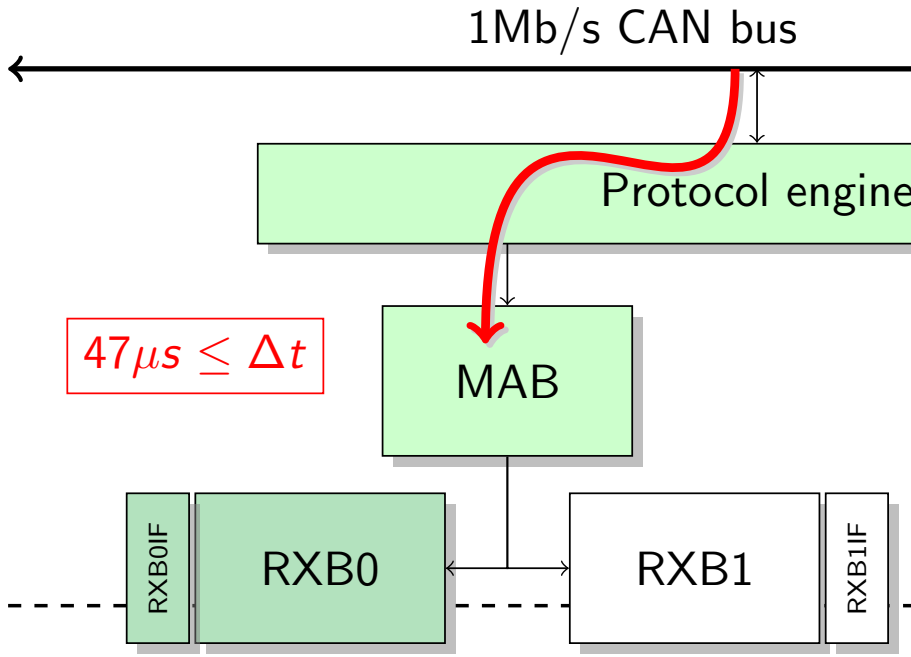
Si Δt n'est pas connu ?



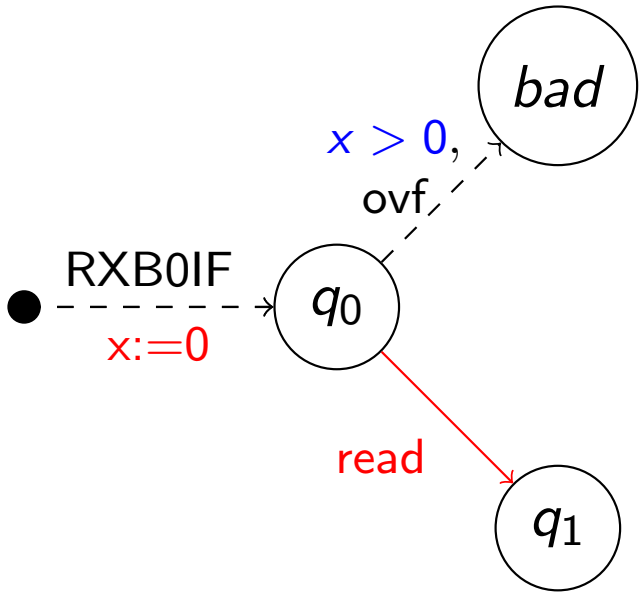
Application to device drivers : avoidable actions

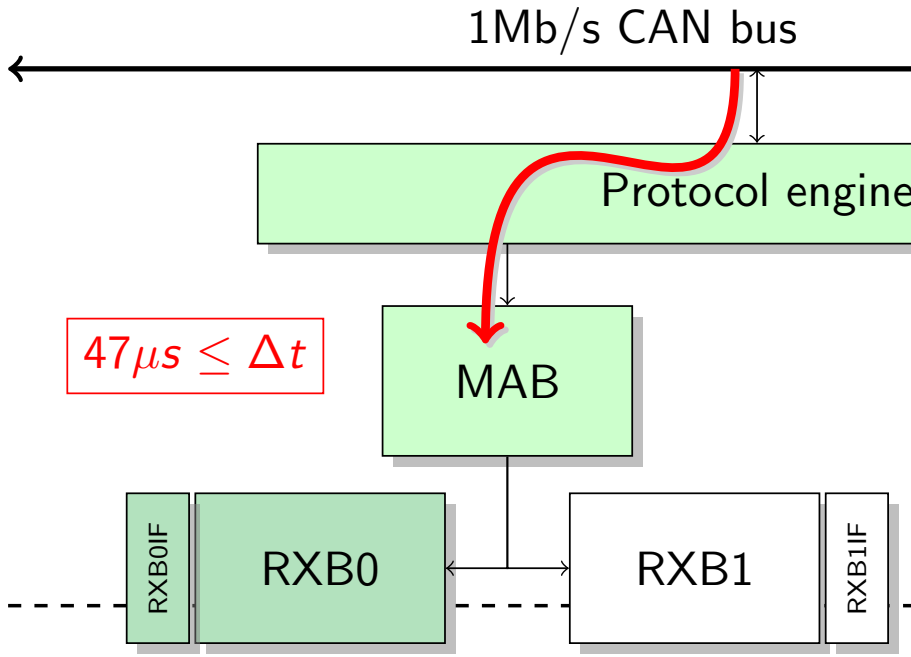


Si Δt n'est pas connu ?



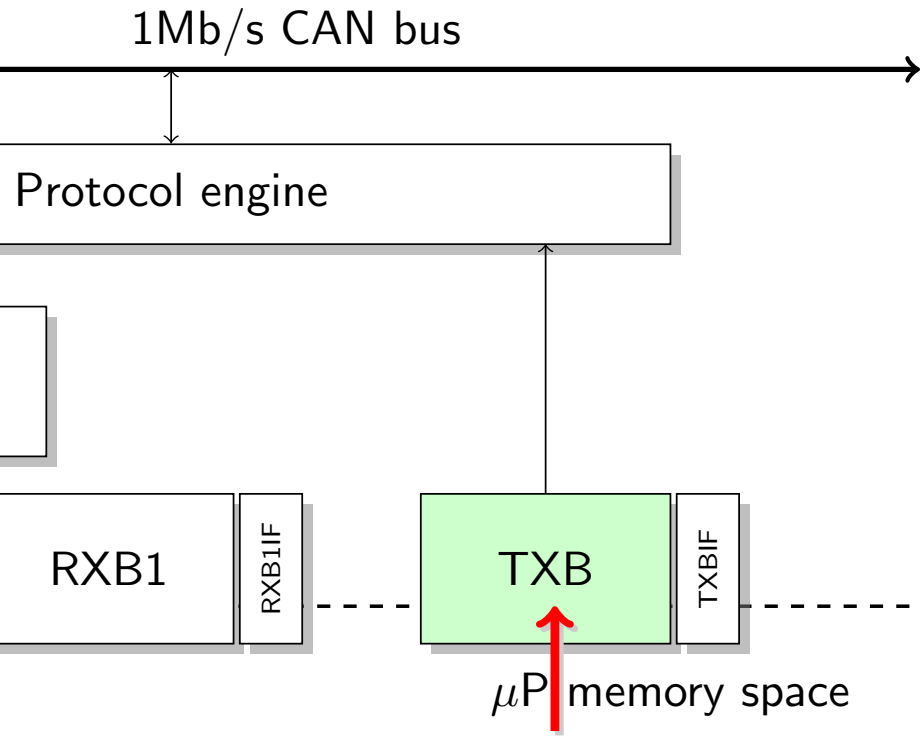
Application to device drivers : avoidable actions

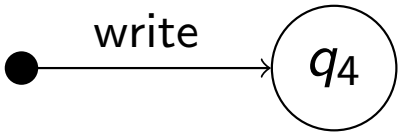




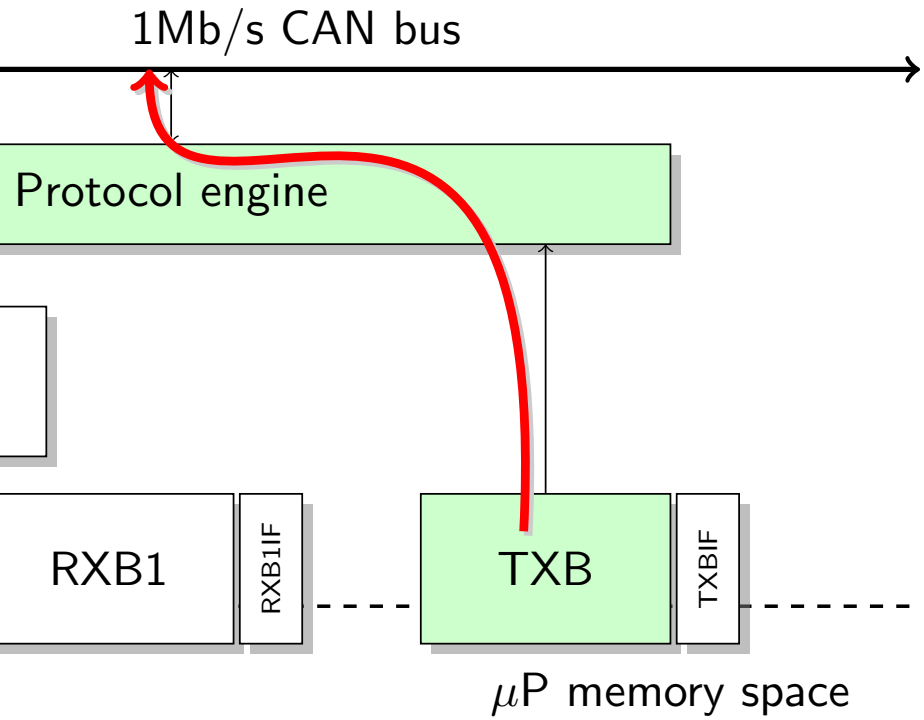
ovf est évitable (non immédiate)
read est urgente

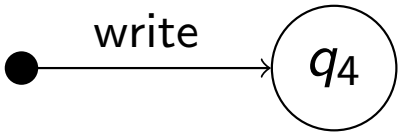
Application to device drivers : ineluctable actions



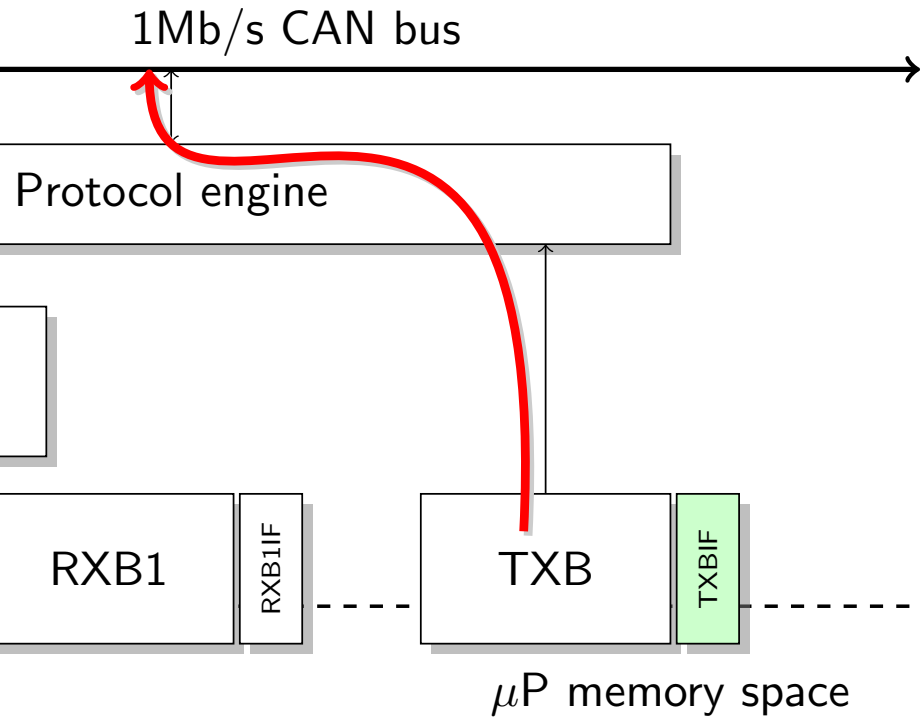


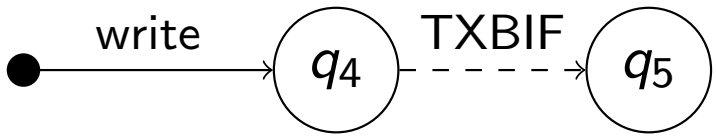
Application to device drivers : ineluctable actions



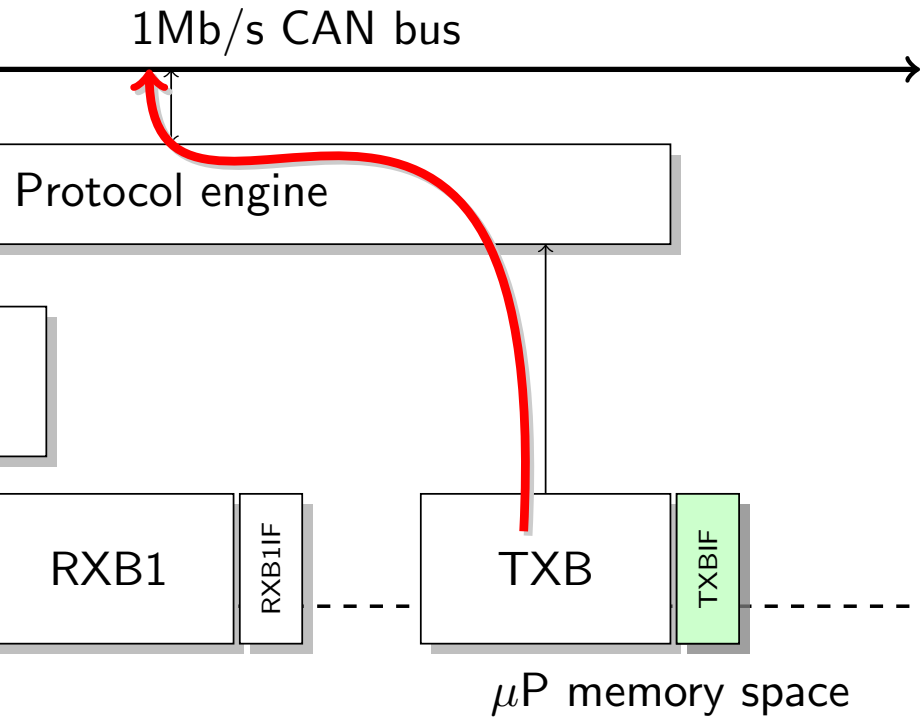


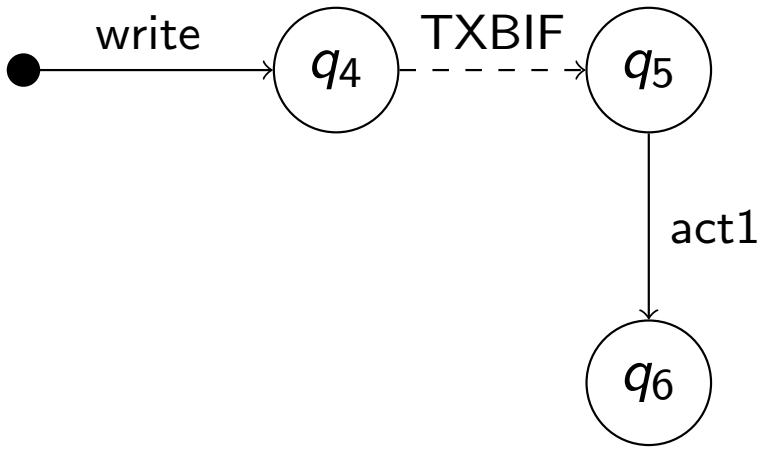
Application to device drivers : ineluctable actions



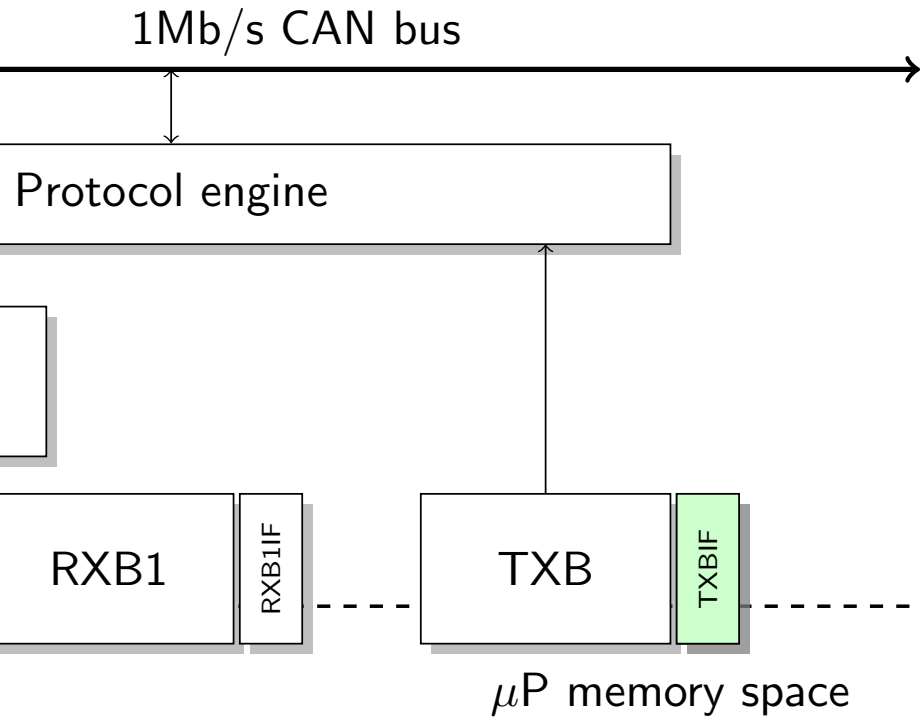


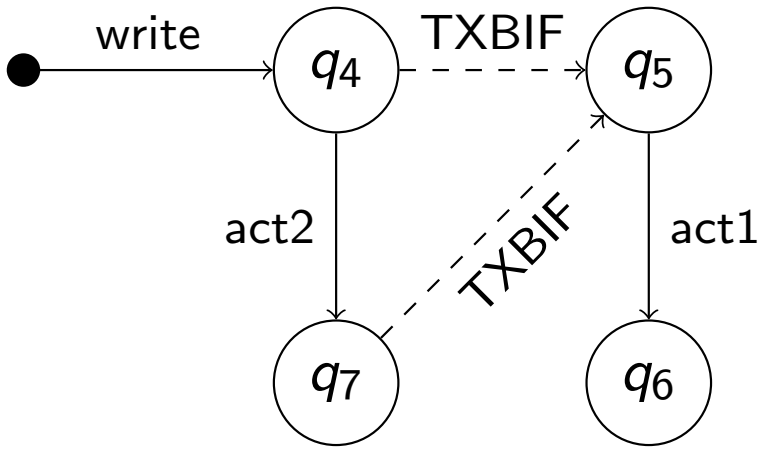
Application to device drivers : ineluctable actions



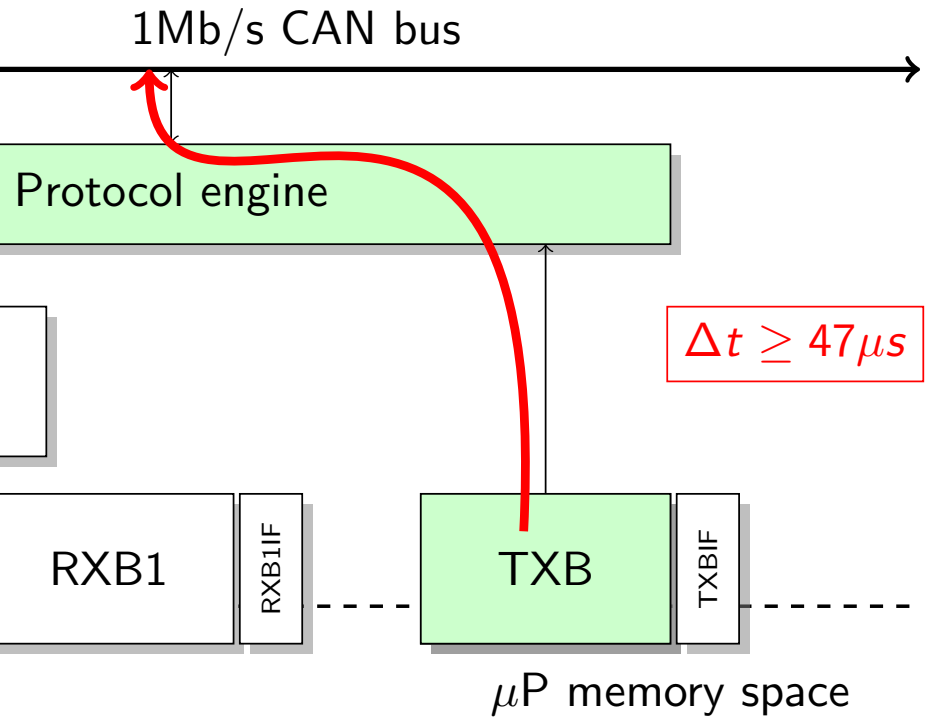


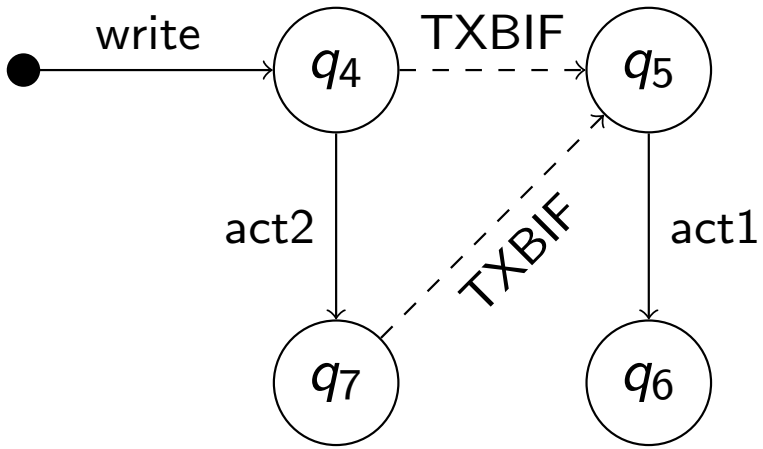
Application to device drivers : ineluctable actions



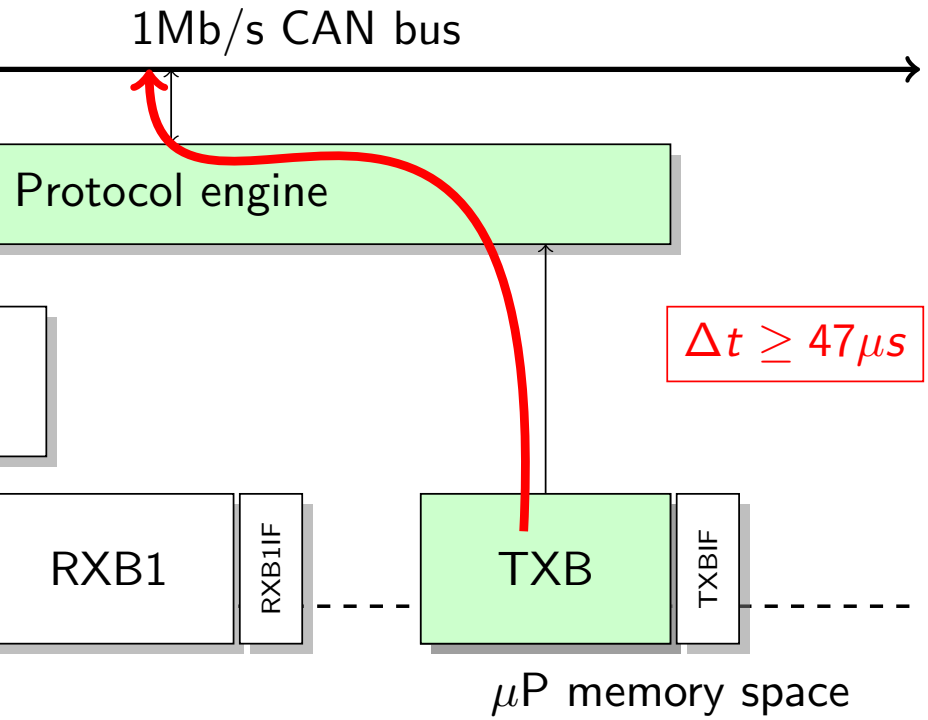


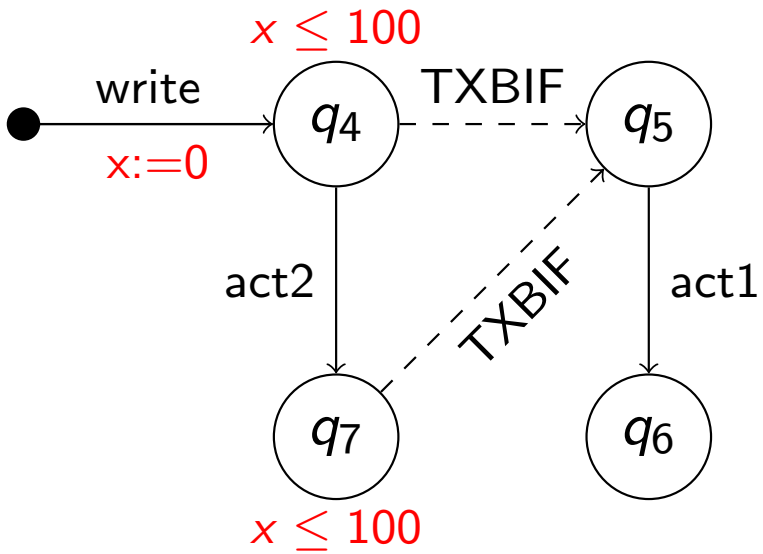
Application to device drivers : ineluctable actions



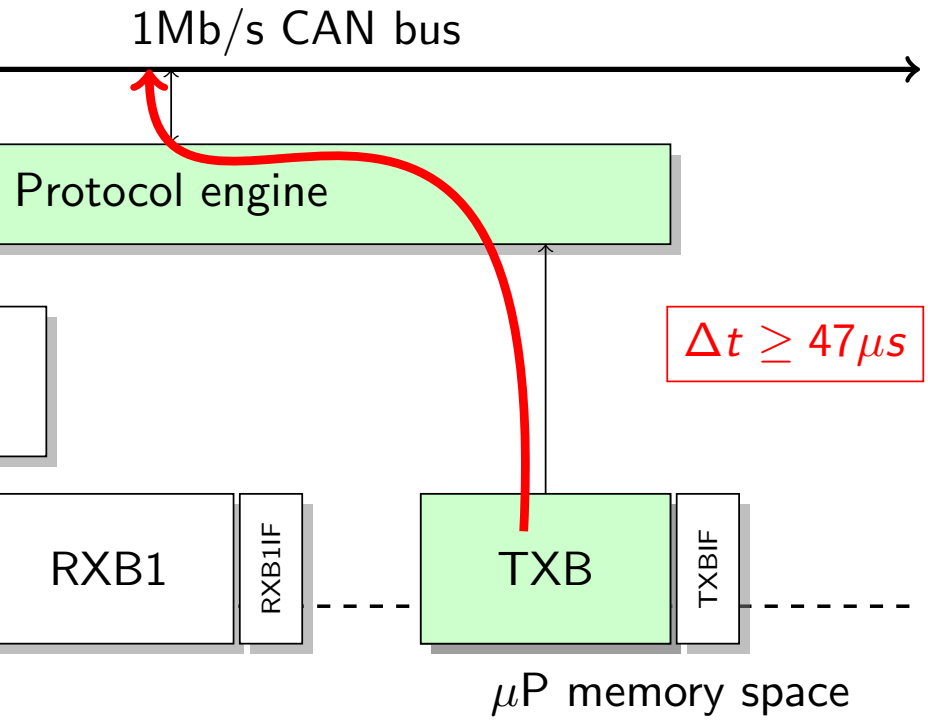


Application to device drivers : ineluctable actions

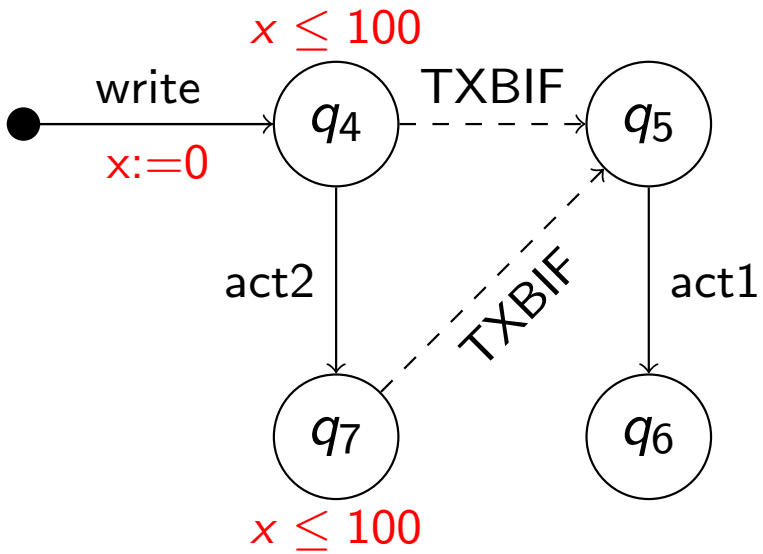




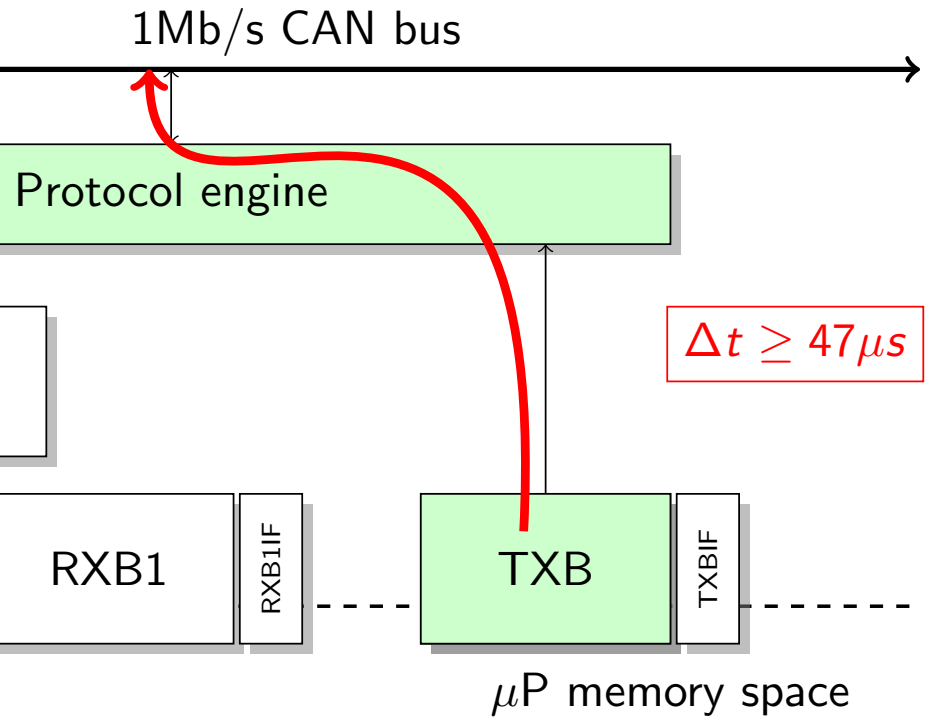
Application to device drivers : ineluctable actions



Jeu temporisé avec invariant

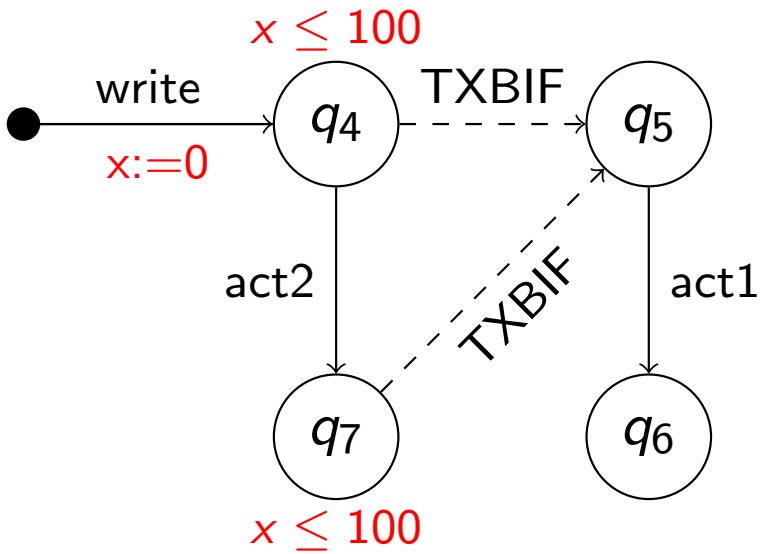


Application to device drivers : ineluctable actions

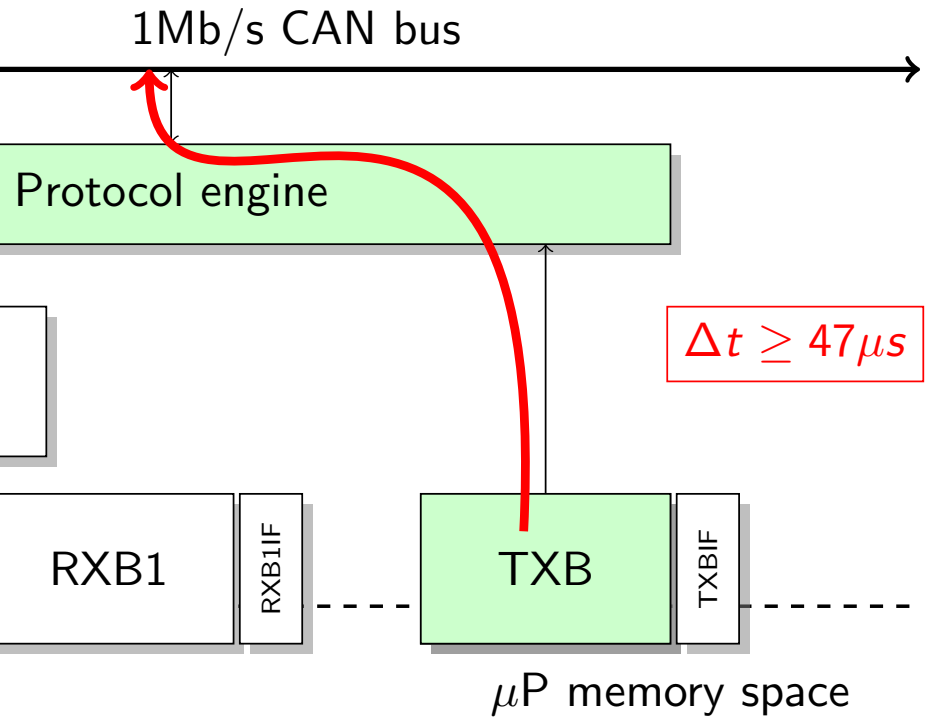


Pourquoi 100 ?

Jeu temporisé avec invariant



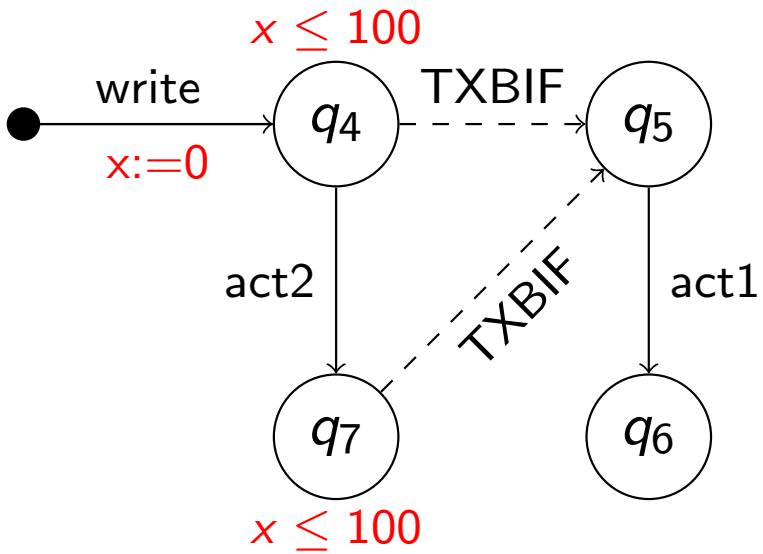
Application to device drivers : ineluctable actions



TXBIF est inéluctable

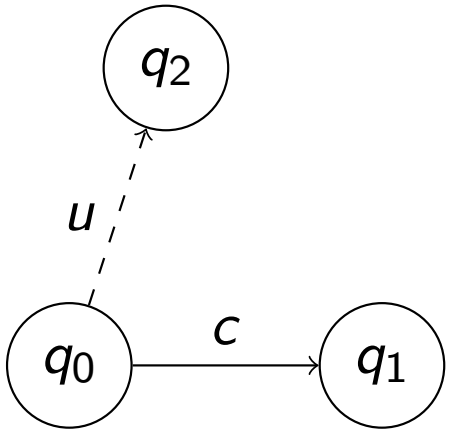
Pourquoi 100 ?

Jeu temporisé avec invariant



Structure de jeu

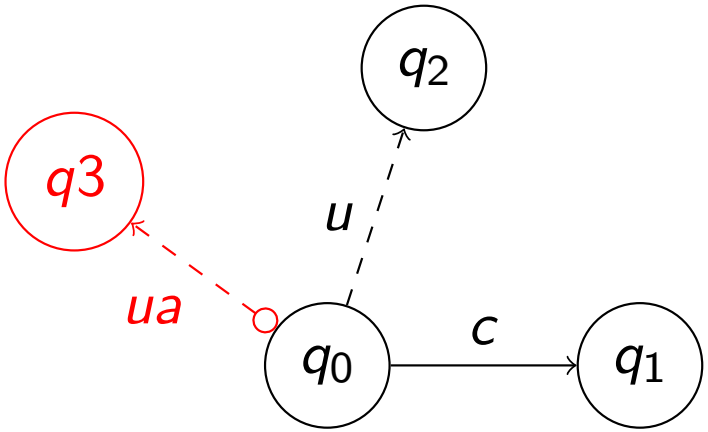
$$\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$$



- $\mathbf{c} \in A_C$ contrôlable
- $\mathbf{u} \in A_U$ incontrôlable

Structure de jeu

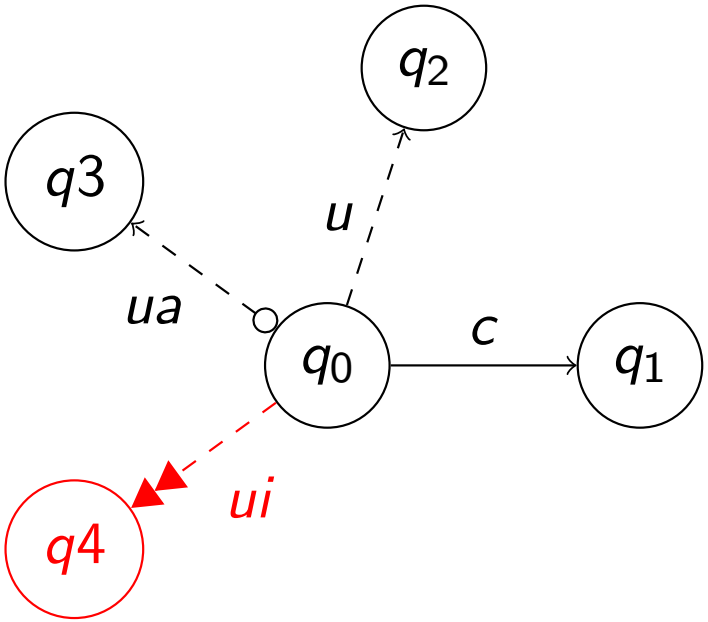
$$\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$$



- **c** $\in A_C$ contrôlable
- **u** $\in A_U$ incontrôlable
- **ua** $\in A_U^\star$ incontrôlable et non immédiate : évitable

Structure de jeu

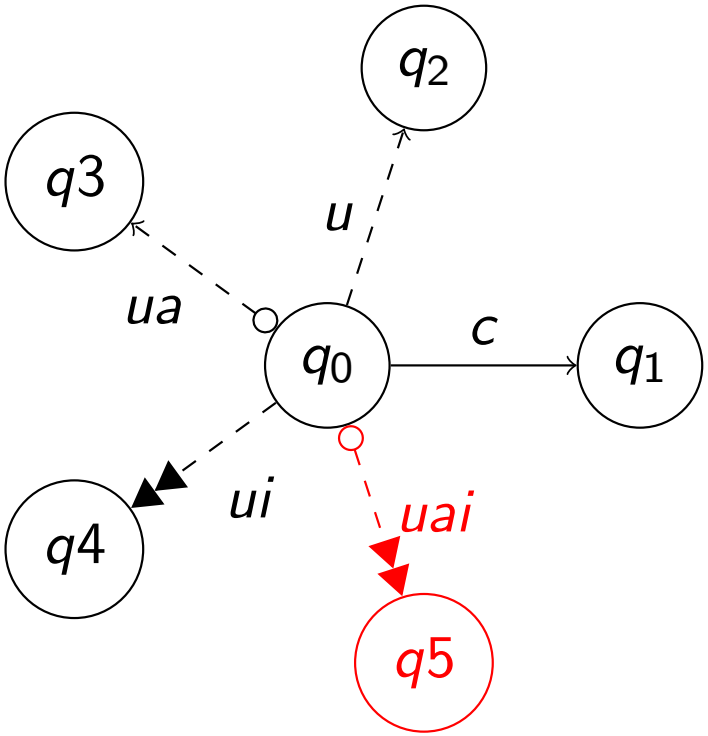
$$\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$$



- **c** $\in A_C$ contrôlable
- **u** $\in A_U$ incontrôlable
- **ua** $\in A_U^\star$ incontrôlable et non immédiate : évitable
- **ui** $\in A_U^\diamond$ incontrôlable et inéluctable;

Structure de jeu

$$\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$$



- **c** $\in A_C$ contrôlable
- **u** $\in A_U$ incontrôlable
- **ua** $\in A_U^{\star}$ incontrôlable et non immédiate : évitable
- **ui** $\in A_U^{\diamond}$ incontrôlable et inéluctable;
- **uai** $\in A_U^{\diamond\star}$ incontrôlable, évitable and inéluctable

Stratégie

Soit $\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$, une structure de jeu
Soit $\Delta = \{\mathbf{0}, \overline{\mathbf{0}}, \bullet\}$

Definition (Stratégie *sans mémoire* s_i pour un joueur $i \in \{C, U\}$)

$s_i : Q \to 2^{(A_i \times \Delta)}$ telle que $\langle a, d \rangle \in s_i(q) \Rightarrow a \in A_i$, $d \in \Delta$ et $q \xrightarrow{a} q' \in \delta$

Stratégie

Soit $\mathcal{G} = (Q, q_0, A_C, A_U, \delta)$, une structure de jeu
Soit $\Delta = \{\mathbf{0}, \overline{\mathbf{0}}, \bullet\}$

Definition (Stratégie *sans mémoire* s_i pour un joueur $i \in \{C, U\}$)

$s_i : Q \to 2^{(A_i \times \Delta)}$ telle que $\langle a, d \rangle \in s_i(q) \Rightarrow a \in A_i$, $d \in \Delta$ et $q \xrightarrow{a} q' \in \delta$

Definition (Stratégies avec actions inéluctables et évitables)

Soit $s_U : Q \to 2^{(A_U \times \Delta)}$, une stratégie de l'environnement. $\forall q \in Q$,

- si il existe $q \xrightarrow{a} q'$ avec $a \in A_U^{\diamond}$ (i.e. ineluctable) alors $s_U(q) \neq \emptyset$.
- si il existe $q \xrightarrow{a} q'$ avec $a \in A_U^{\star}$ (i.e. évitable) et si $\langle a, d \rangle \in s_U(q)$ avec $d \in \Delta$ alors $d = \overline{\mathbf{0}}$.

Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:

q

Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:

$$q \xrightarrow{\langle c_0, d \in \Delta \rangle} q_1$$

si $\langle c_0, d \rangle \in s_C(q)$

Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:

$$q \xrightarrow{\langle c_0, d \in \Delta \rangle} q_1 \xrightarrow{\langle u_1, d \in \Delta \rangle} q_2$$

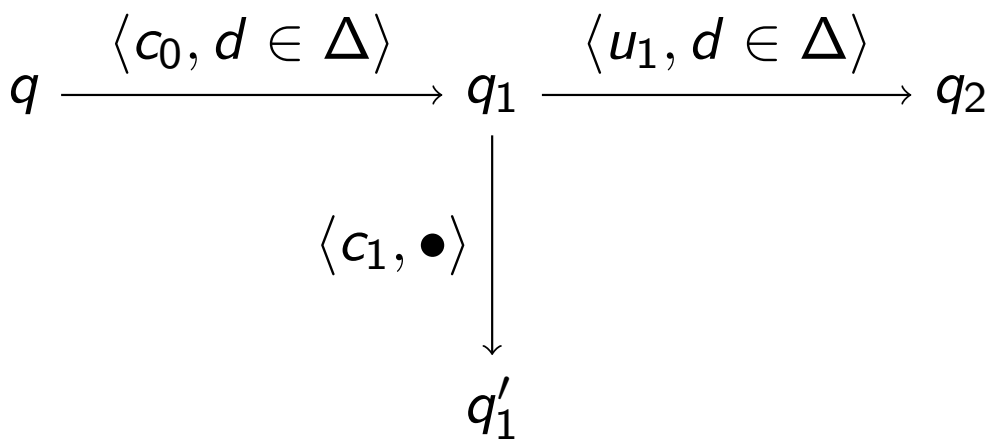
Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:



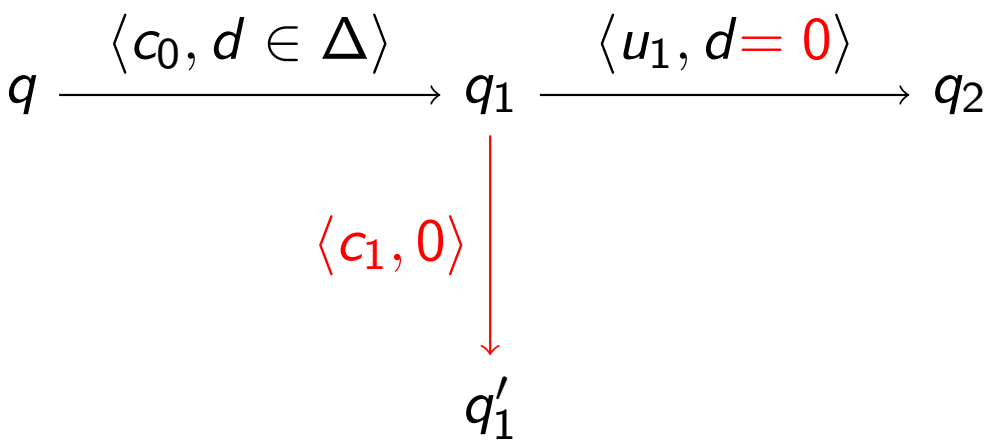
Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:



Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:

$$q \xrightarrow{\langle c_0, d \in \Delta \rangle} q_1 \xrightarrow{\langle u_1, d \in \Delta \rangle} q_2$$

Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:

$$q \xrightarrow{\langle c_0, d \in \Delta \rangle} q_1 \xrightarrow{\langle u_1, d \in \Delta \rangle} q_2 \xrightarrow{\langle u_2, \overline{0} \rangle} q_3$$

si $u_2 \in A_U^\star$

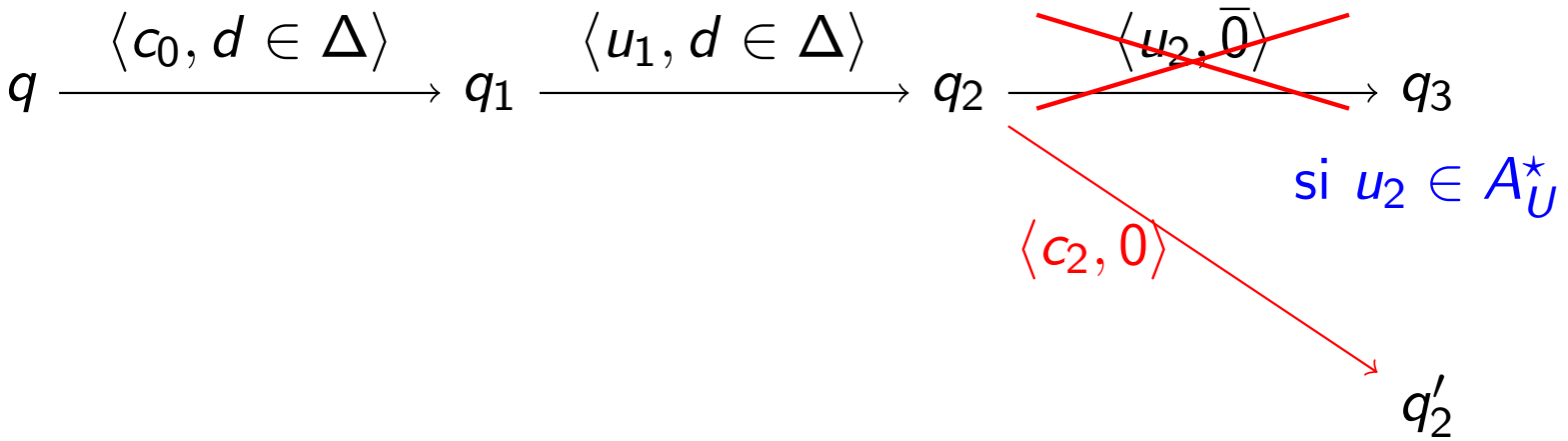
Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:



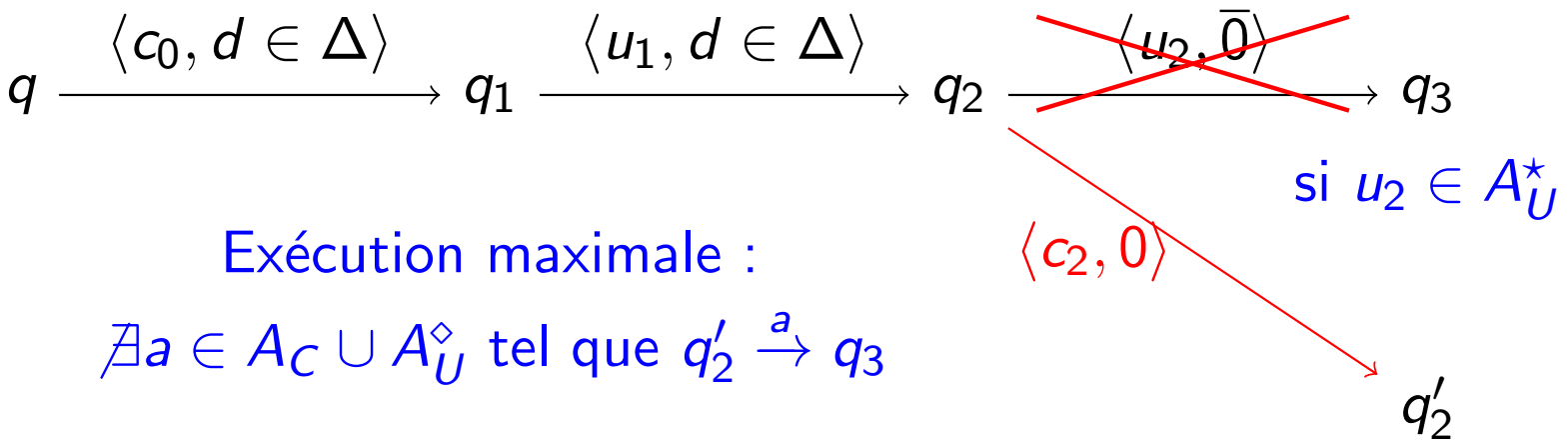
Outcome

Definition (Exécution)

Une *exécution* est une séquence $q_0 \xrightarrow{\langle a_1, d_1 \rangle} q_1 \xrightarrow{\langle a_2, d_2 \rangle} \dots$ avec $a_i \in A_C \cup A_U$, $d_i \in \Delta$, et $q_i \in Q$.

Definition (Résultats de l'application de la stratégie)

Soit s_C, une stratégie pour le contrôleur. Le *résultat* $Outcome(q, s_C)$ de s_C à partir de l'état q est le sous-ensemble des exécutions défini par:



Stratégie gagnante

$(\mathcal{G}, C_{\mathcal{W}})$ est un *jeu* défini par

- $\mathcal{G}$, une structure de jeu.
- Une condition gagnante $C_{\mathcal{W}}$: un ensemble d'exécutions autorisées.

Stratégie gagnante

$(\mathcal{G}, C_{\mathcal{W}})$ est un *jeu* défini par

- $\mathcal{G}$, une structure de jeu.
- Une condition gagnante $C_{\mathcal{W}}$: un ensemble d'exécutions autorisées.

Definition (Stratégie gagnante)

Une stratégie s_C pour le contrôleur est gagnante à partir de l'état q_0 si $\mathit{MaxOutcome}(q_0, s_C) \subseteq C_{\mathcal{W}}$.

Stratégie gagnante

$(\mathcal{G}, C_{\mathcal{W}})$ est un *jeu* défini par

- $\mathcal{G}$, une structure de jeu.
- Une condition gagnante $C_{\mathcal{W}}$: un ensemble d'exécutions autorisées.

Definition (Stratégie gagnante)

Une stratégie s_C pour le contrôleur est gagnante à partir de l'état q_0 si $\mathit{MaxOutcome}(q_0, s_C) \subseteq C_{\mathcal{W}}$.

Problème

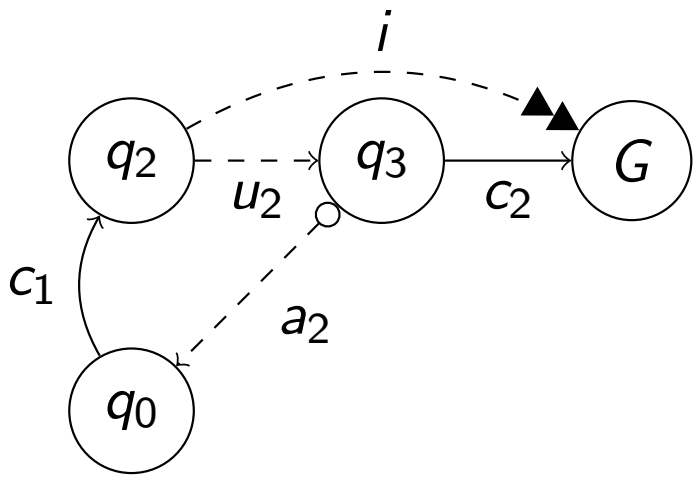
Calculer une stratégie gagnante

- sans mémoire
- pour un jeu d'accessibilité, de sûreté ou d'accessibilité sûre

Prédécésseurs contrôlables

Prédécésseurs contrôlables

$$\pi(X) = \mathrm{pre}_{A_C}(X) \setminus \mathrm{pre}_{A_U^{\star}}(\overline{X}) \cup \mathrm{pre}_{A_U^{\diamond}}(X) \setminus \mathrm{pre}_{A_U}(\overline{X})$$



Exemple X = {G}

- $\mathrm{pre}_{A_C}(X) = \{q_3\}$
- $\mathrm{pre}_{A_U^{\diamond}}(X) = \{q_2\}$
- $\pi(X) = \{q_3\}$

$\overline{X} = \{q_0, q_2, q_3\}$

- $\mathrm{pre}_{A_U^{\star}}(\overline{X}) = \{q_2\}$
- $\mathrm{pre}_{A_U}(\overline{X}) = \{q_2, q_3\}$

Jeu d'accessibilité

L'objectif est d'atteindre un état de Goal

Point fixe en arrière : $\mathcal{W}$

$\mathcal{W}_0 = \text{Goal}$ and
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n)$

Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\overline{\star}}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu d'accessibilité

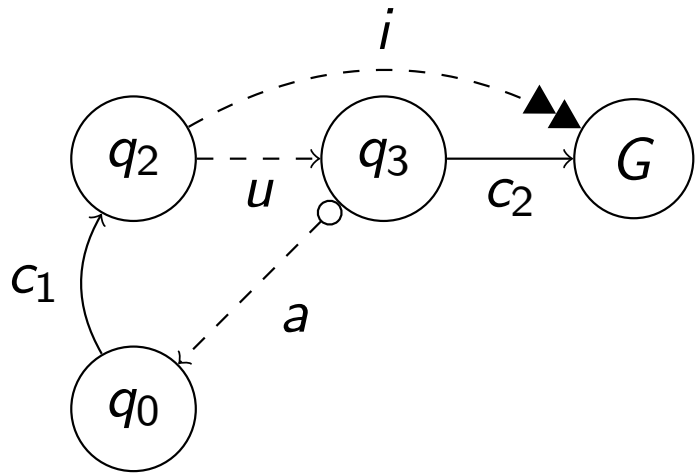
L'objectif est d'atteindre un état de Goal

Point fixe en arrière : $\mathcal{W}$

$\mathcal{W}_0 = \text{Goal and}$
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n)$

Exemple

$\mathcal{W}_0 = \{G\}$
$\mathcal{W}_1 = \{G, q_3\}$
$\mathcal{W}_2 = \{G, q_3, q_2\}$
$\mathcal{W}_3 = \{G, q_3, q_2, q_0\}$
$\mathcal{W} = \mathcal{W}_3$



Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\overline{\star}}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu d'accessibilité

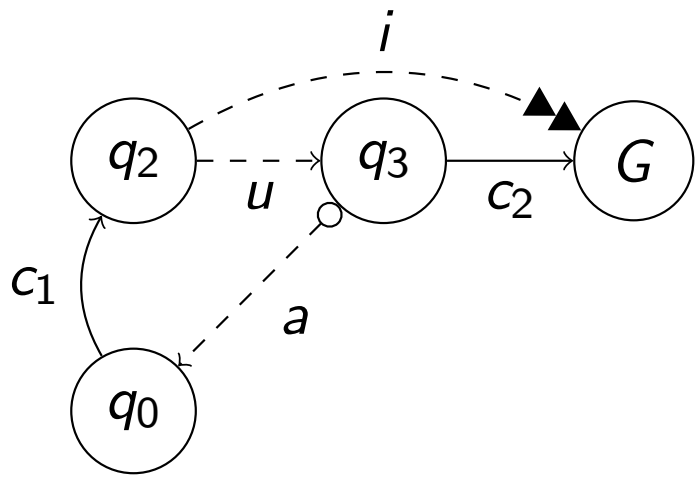
L'objectif est d'atteindre un état de Goal

Point fixe en arrière : $\mathcal{W}$

$\mathcal{W}_0 = \text{Goal and}$
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n)$

Exemple

$\mathcal{W}_0 = \{G\}$
$\mathcal{W}_1 = \{G, q_3\}$
$\mathcal{W}_2 = \{G, q_3, q_2\}$
$\mathcal{W}_3 = \{G, q_3, q_2, q_0\}$
$\mathcal{W} = \mathcal{W}_3$



Stratégie sans mémoire

$s(q_0) = \{\langle c_1, \bullet \rangle\}$
$s(q_2) = \emptyset$
$s(q_3) = \{\langle c_2, \mathbf{0} \rangle\}$

Jeu de sûreté

L'objectif est de rester dans un ensemble d'états Safe

Point fixe en arrière: $\mathcal{W}$

$\mathcal{W}_0 = \text{Safe and}$
$\mathcal{W}_{n+1} = \mathcal{W}_n \cap \pi(\mathcal{W}_n)$

Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\overline{\star}}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu de sûreté

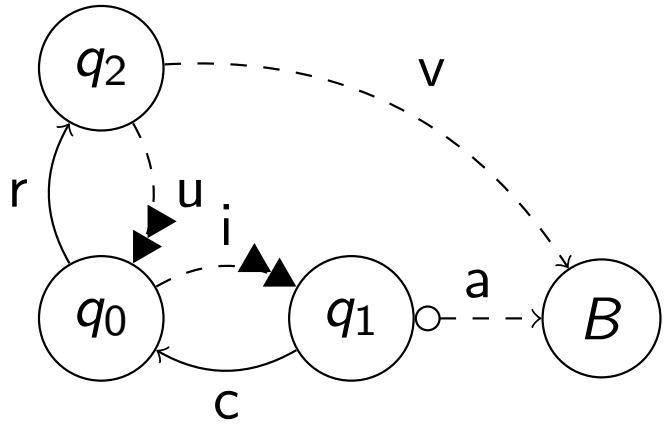
L'objectif est de rester dans un ensemble d'états Safe

Point fixe en arrière: $\mathcal{W}$

$\mathcal{W}_0 = \text{Safe and}$
$\mathcal{W}_{n+1} = \mathcal{W}_n \cap \pi(\mathcal{W}_n)$

Exemple

$\mathcal{W}_0 = \{q_0, q_1, q_2\}$
$\text{pre}_{A_C}(\mathcal{W}_0) = \{q_0, q_1\}$
$\text{pre}_{A_U^{\overline{\star}}}(B) = \{q_2\}$
$\text{pre}_{A_U^{\diamond}}(\mathcal{W}_0) = \{q_1, q_2\}$
$\text{pre}_{A_U}(B) = \{q_1, q_2\}$
$\mathcal{W}_1 = \{q_0, q_1\}$
$\mathcal{W} = \mathcal{W}_1$



Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\overline{\star}}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu de sûreté

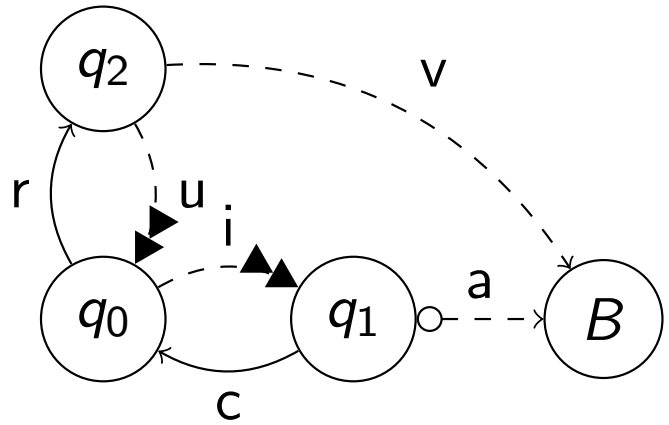
L'objectif est de rester dans un ensemble d'états Safe

Point fixe en arrière: $\mathcal{W}$

$\mathcal{W}_0 = \text{Safe and}$
$\mathcal{W}_{n+1} = \mathcal{W}_n \cap \pi(\mathcal{W}_n)$

Exemple

$\mathcal{W}_0 = \{q_0, q_1, q_2\}$
$\text{pre}_{A_C}(\mathcal{W}_0) = \{q_0, q_1\}$
$\text{pre}_{A_U^{\exists}}(B) = \{q_2\}$
$\text{pre}_{A_U^{\forall}}(\mathcal{W}_0) = \{q_1, q_2\}$
$\text{pre}_{A_U}(B) = \{q_1, q_2\}$
$\mathcal{W}_1 = \{q_0, q_1\}$
$\mathcal{W} = \mathcal{W}_1$



Stratégie sans mémoire la plus permissive

$s(q_0) = \emptyset$
$s(q_1) = \{\langle c, \mathbf{0}\rangle\}$

Jeu d'accessibilité sûre

Atteindre Goal en restant dans Safe

Point fixe en arrière : $\mathcal{W}$

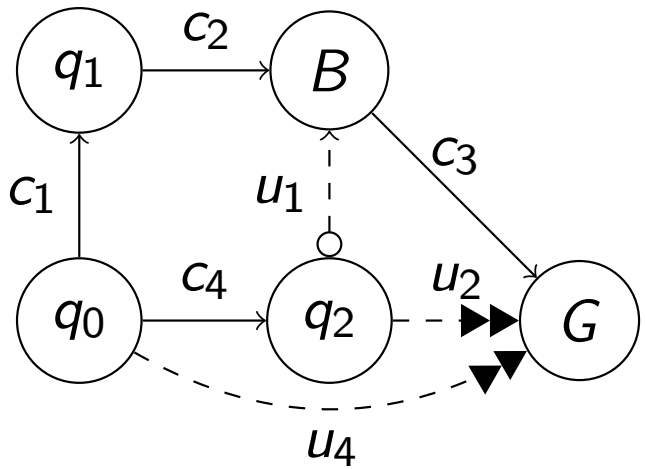
$\mathcal{W}_0 = \text{Goal} \cap \text{Safe}$ and
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n) \cap \text{Safe}$

Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\overline{\star}}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu d'accessibilité sûre

Atteindre Goal en restant dans Safe



Point fixe en arrière : $\mathcal{W}$

$\mathcal{W}_0 = \text{Goal} \cap \text{Safe}$ and
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n) \cap \text{Safe}$

Exemple

$\mathcal{W}_0 = \{G\}$
$\mathcal{W}_1 = \{G, q_0\}$
$\mathcal{W} = \mathcal{W}_1$

Prédécesseurs contrôlables

$$\pi(X) = \text{pre}_{A_C}(X) \setminus \text{pre}_{A_U^{\star}}(\overline{X}) \cup \text{pre}_{A_U^{\diamond}}(X) \setminus \text{pre}_{A_U}(\overline{X})$$

Jeu d'accessibilité sûre

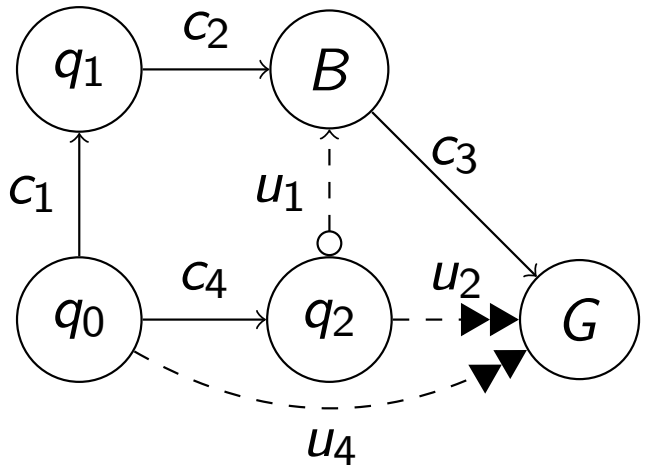
Atteindre Goal en restant dans Safe

Point fixe en arrière : $\mathcal{W}$

$\mathcal{W}_0 = \text{Goal} \cap \text{Safe}$ and
$\mathcal{W}_{n+1} = \mathcal{W}_n \cup \pi(\mathcal{W}_n) \cap \text{Safe}$

Exemple

$\mathcal{W}_0 = \{G\}$
$\mathcal{W}_1 = \{G, q_0\}$
$\mathcal{W} = \mathcal{W}_1$



Stratégie sans mémoire

$s(q_0) = \emptyset$

Résultats

Theorem (Complétude et correction)

$q \in \mathcal{W}$ si et seulement si q est gagnant.

Theorem (Stratégie sans mémoire)

Si le jeu est gagnant alors il est gagnant avec une stratégie sans mémoire.

Complexité

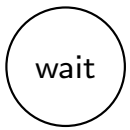
Possible en temps linéaire par rapport au nombre de transitions de l'automate.

Conclusion

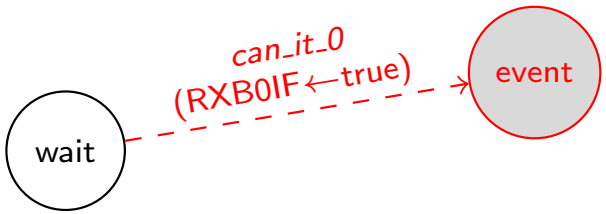
- Extension des automates de jeu avec du temps logique
- Une action *non immédiate* (évitable) ne peut pas se produire instantanément de sorte que le contrôleur peut effectuer en urgence une autre action de manière préventive.
- Une action ineluctable se produira immanquablement et le contrôleur peut donc s'y fier.

- Une partie de l'expressivité des jeux temporisés,
- Simplicité des automates (de jeu) finis
- Implementé dans ROMÉO.
- TODO : Condition de Büchi

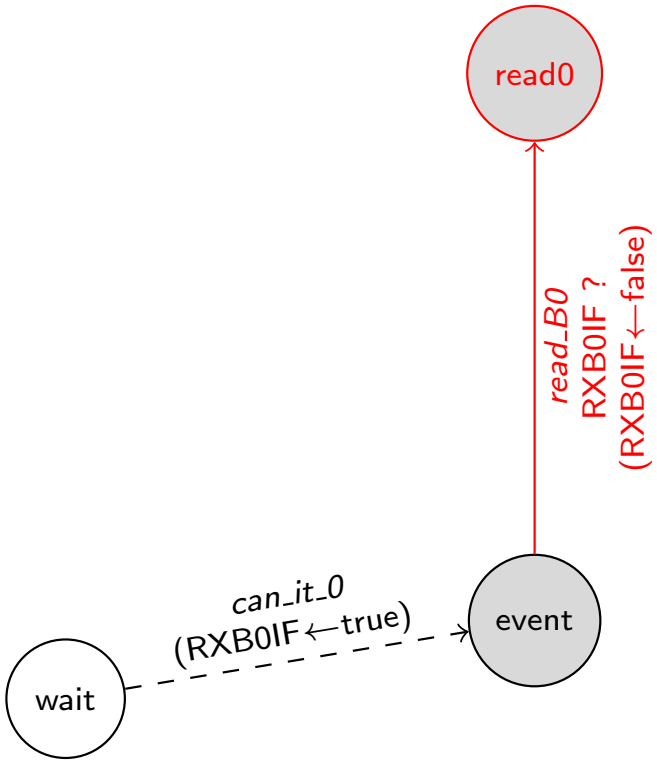
A CAN driver for the PIC18Cxx8



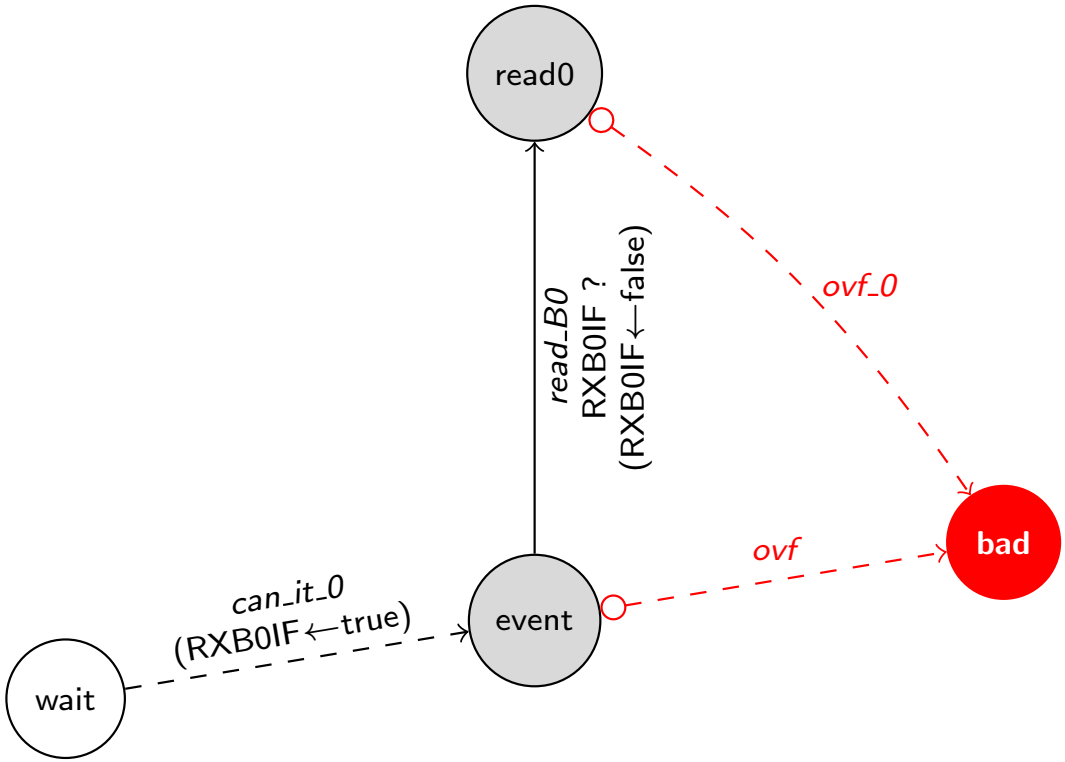
A CAN driver for the PIC18Cxx8



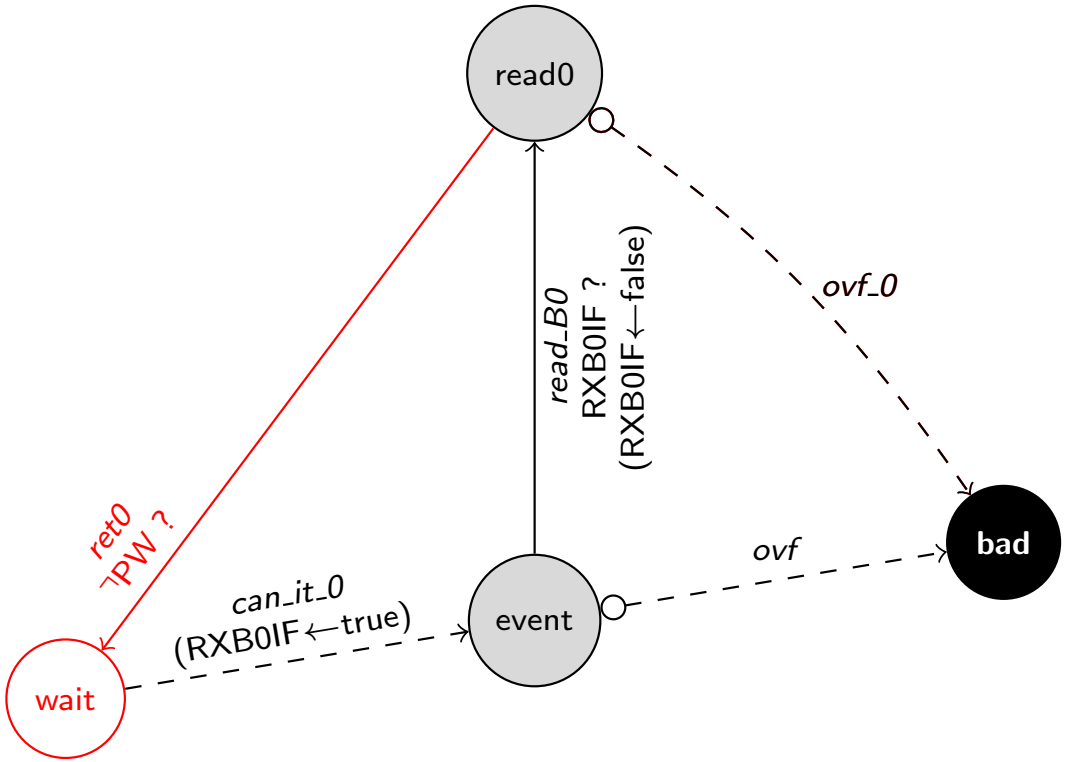
A CAN driver for the PIC18Cxx8



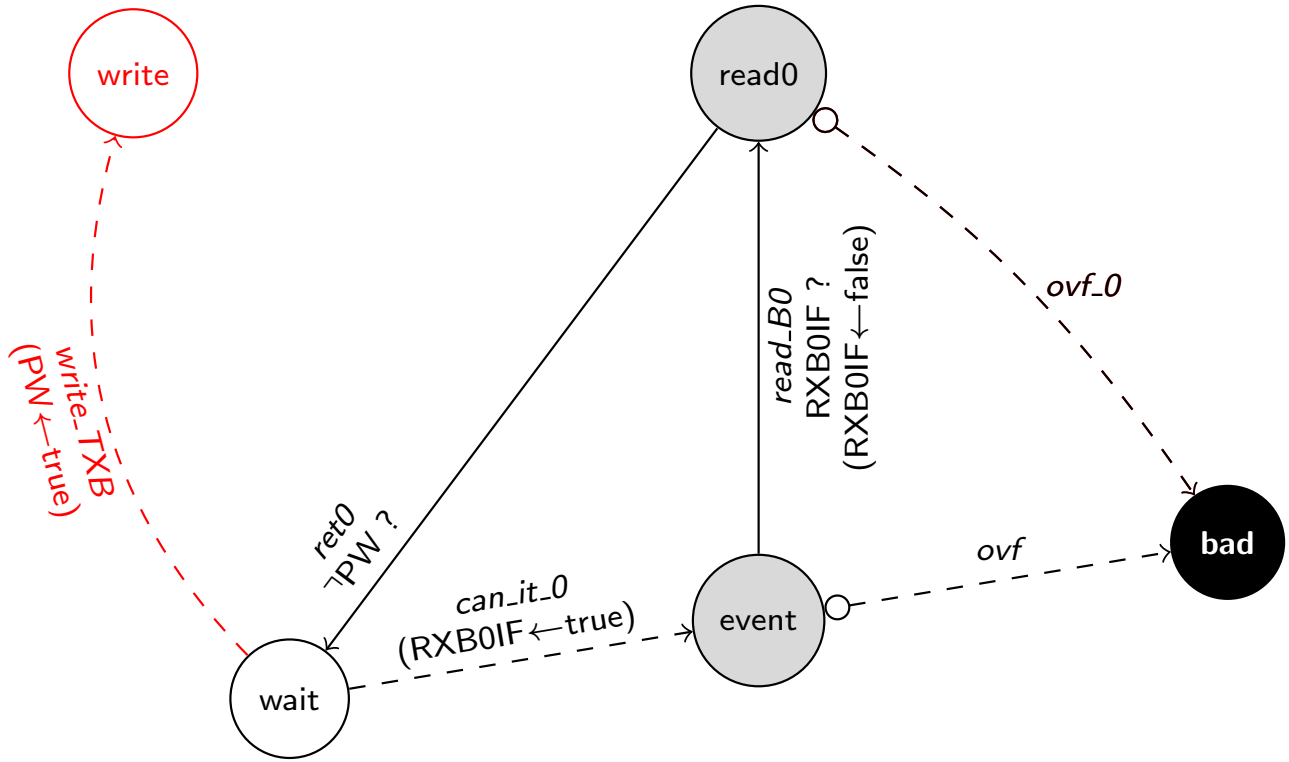
A CAN driver for the PIC18Cxx8



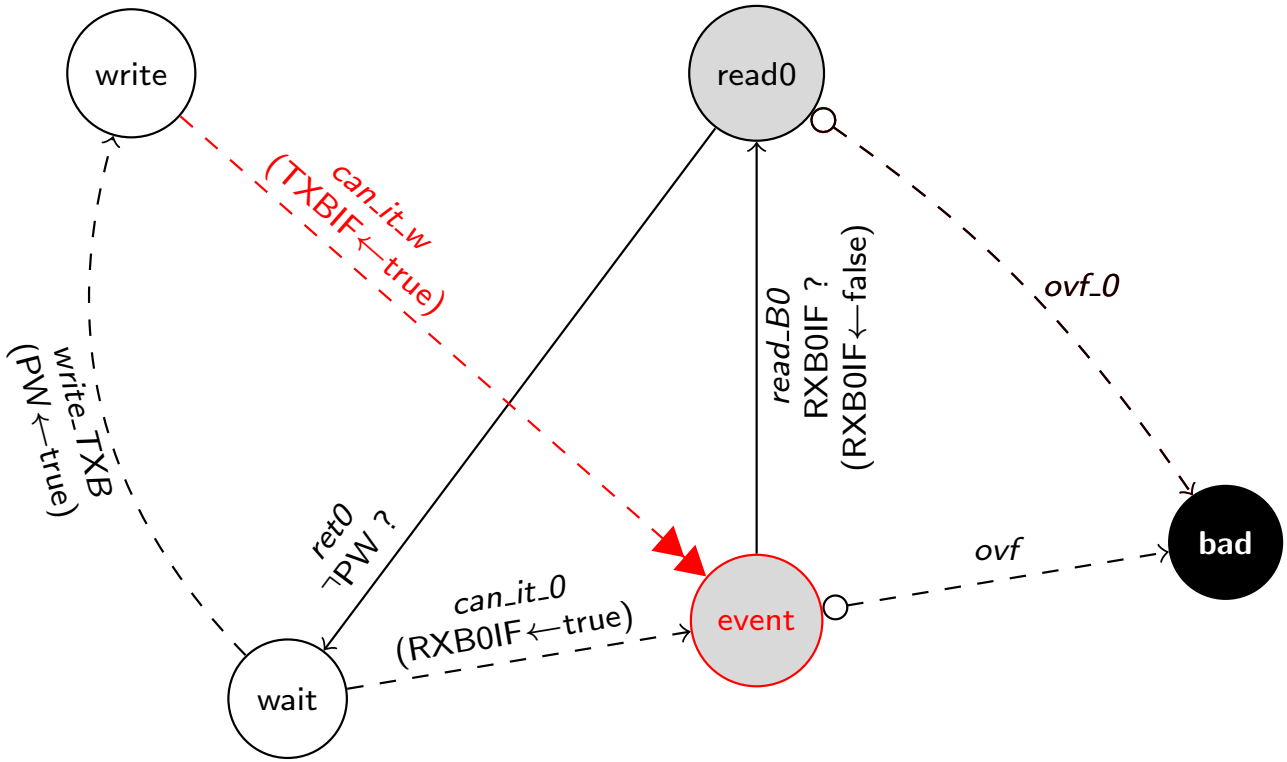
A CAN driver for the PIC18Cxx8



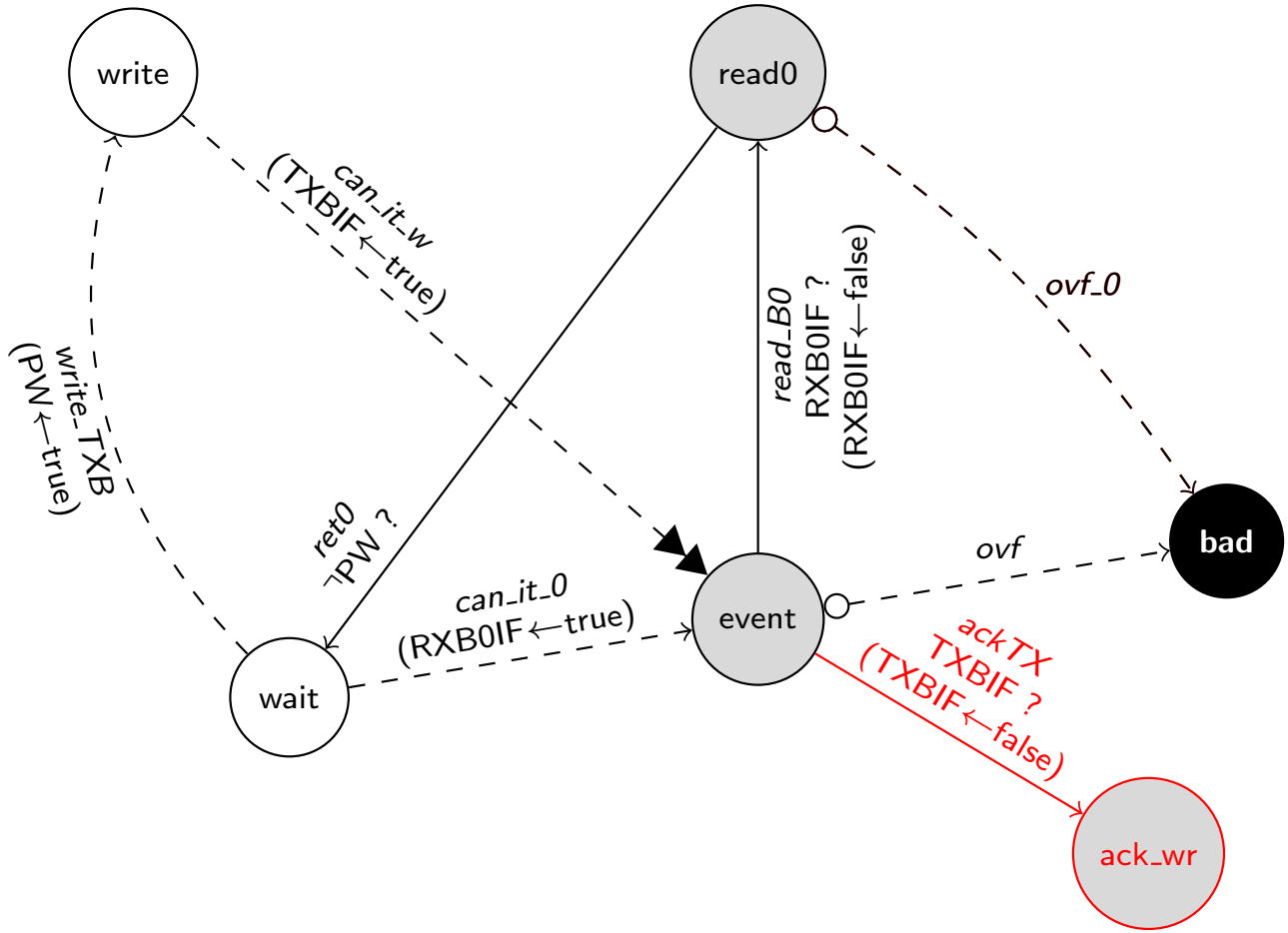
A CAN driver for the PIC18Cxx8



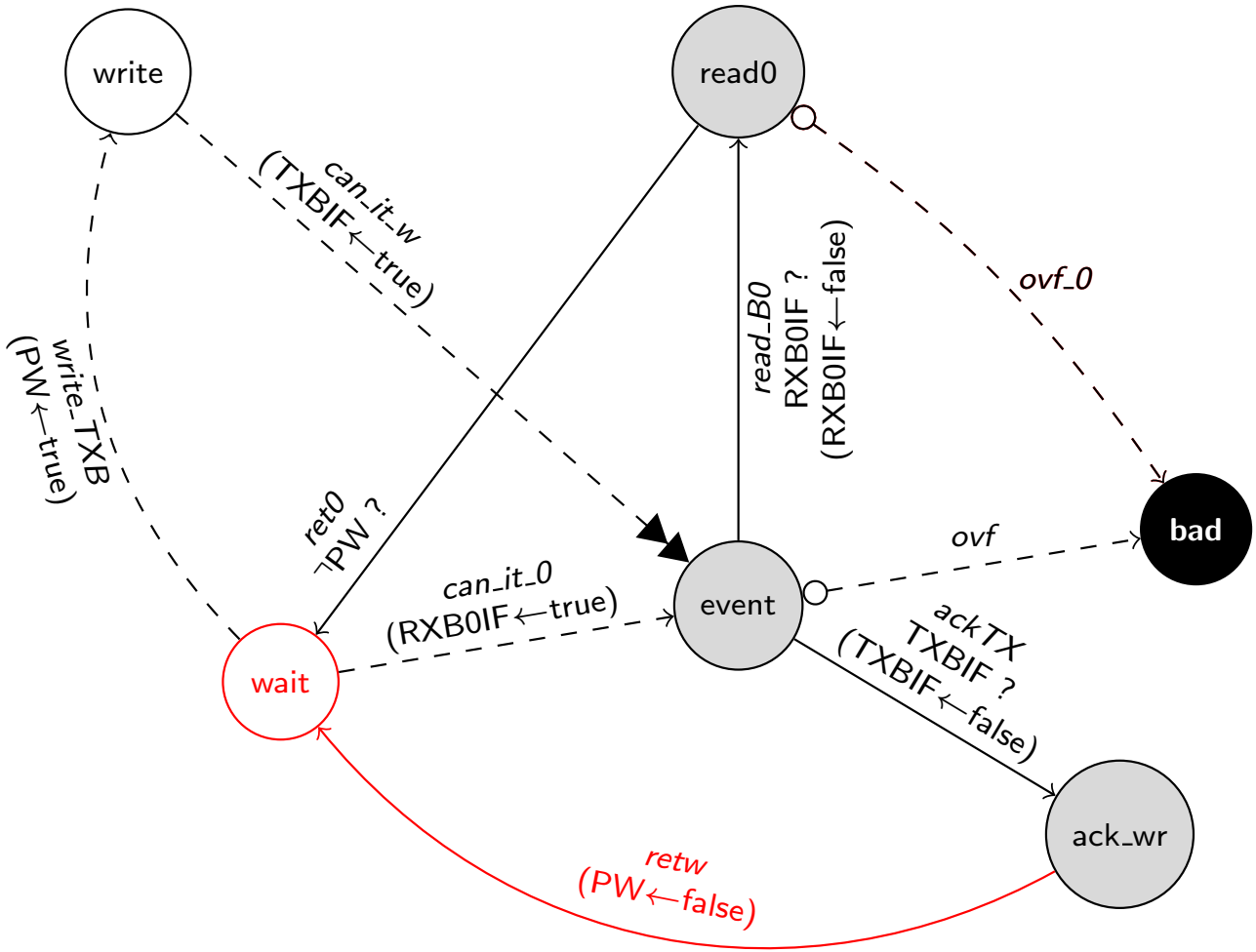
A CAN driver for the PIC18Cxx8



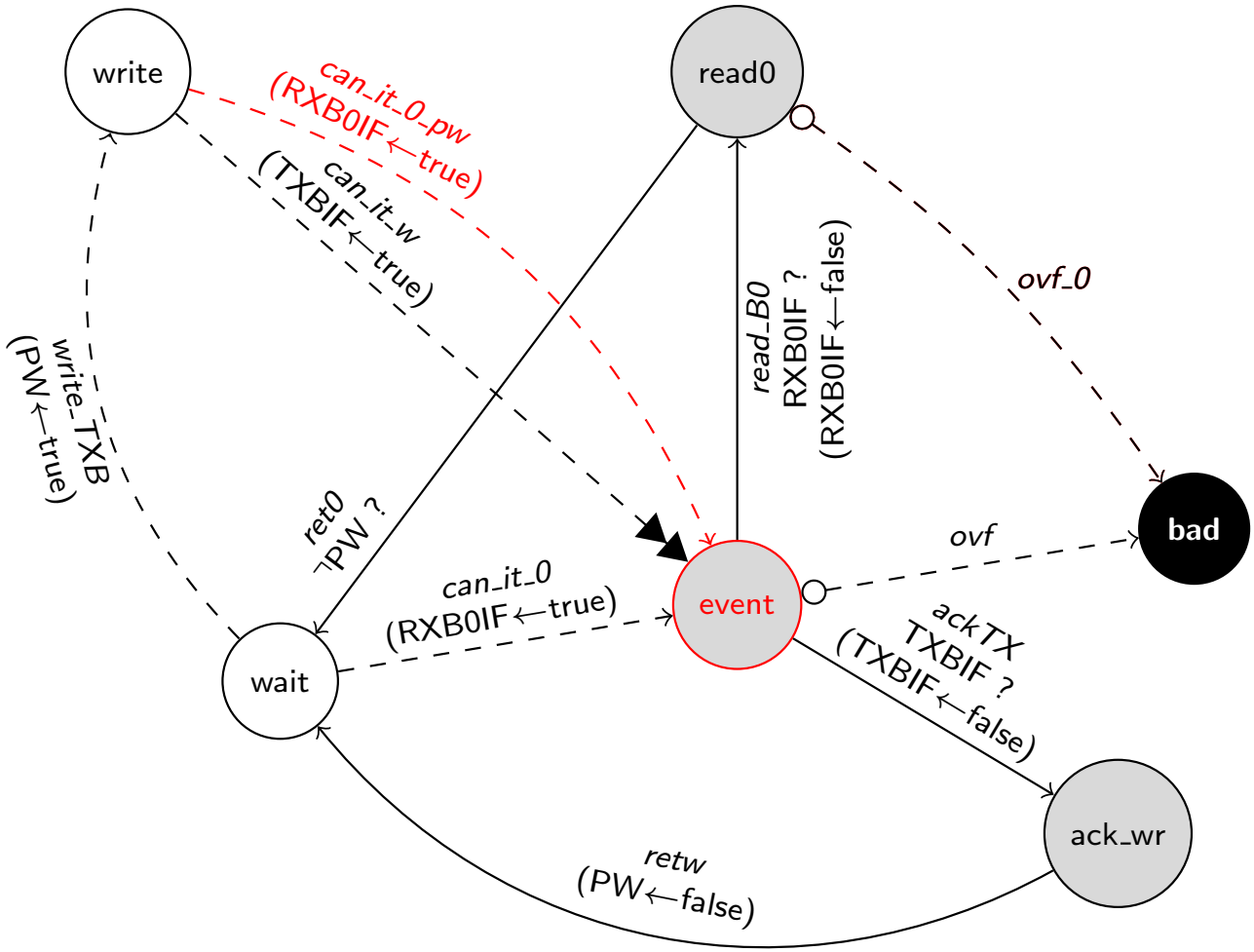
A CAN driver for the PIC18Cxx8



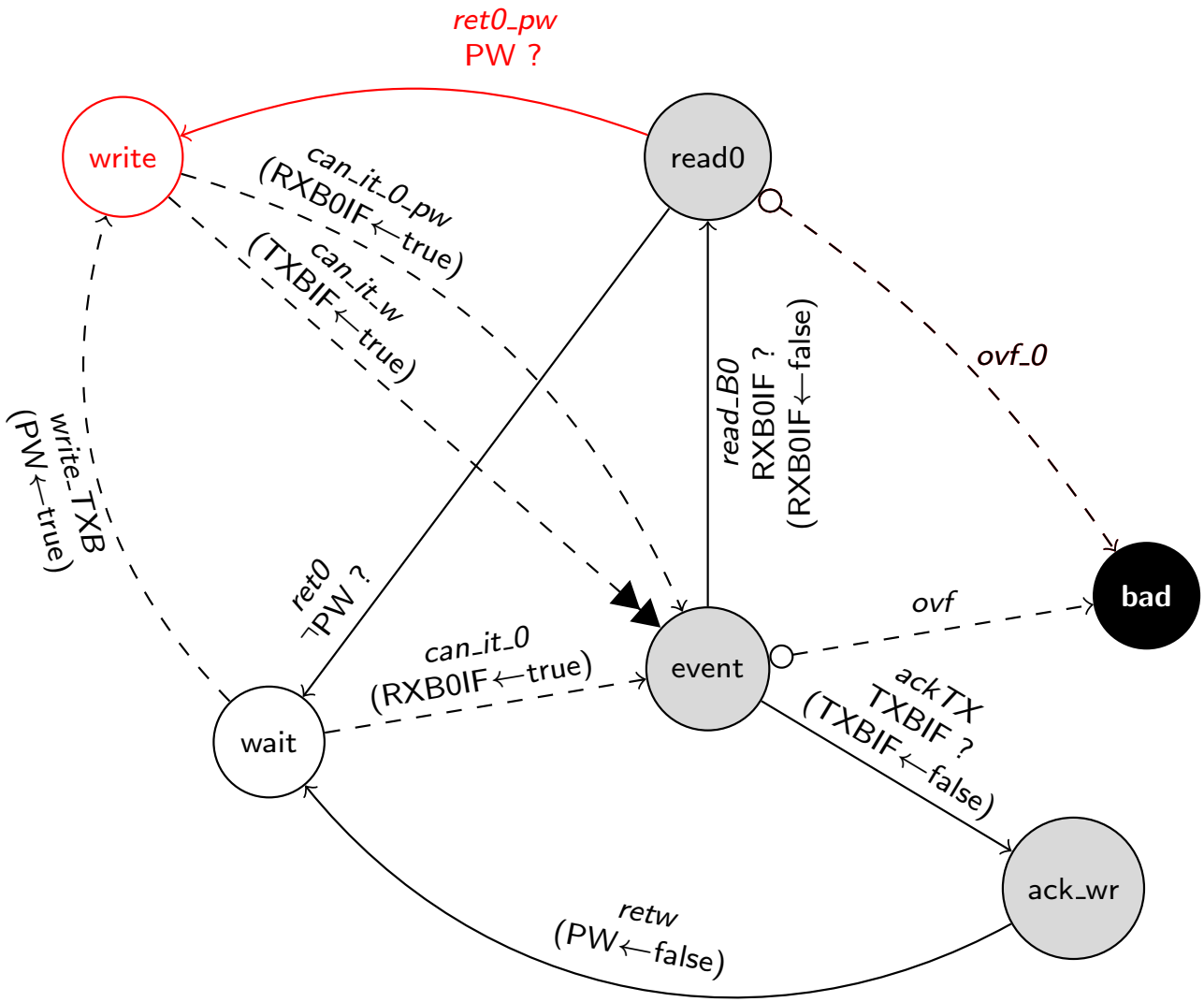
A CAN driver for the PIC18Cxx8



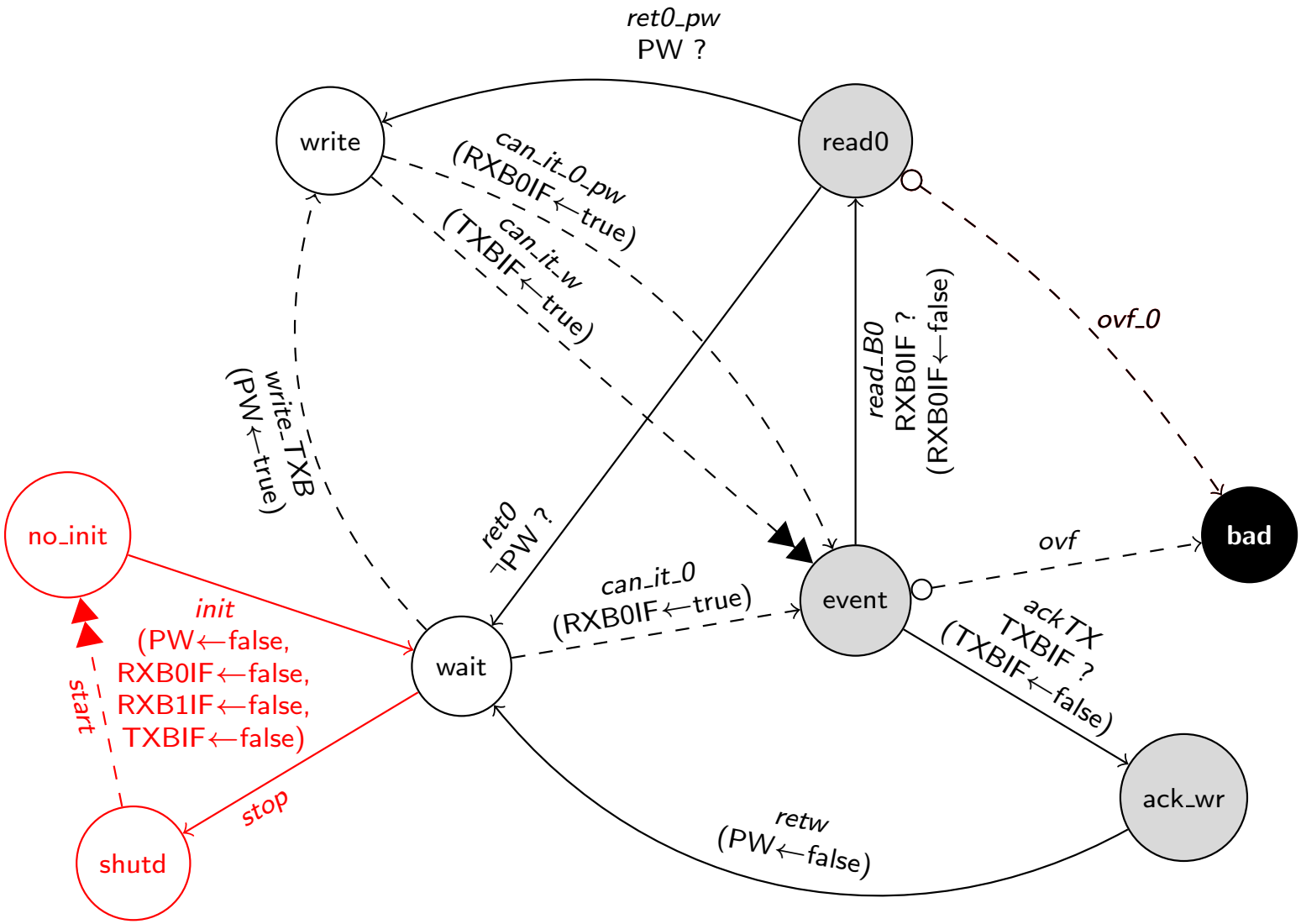
A CAN driver for the PIC18Cxx8



A CAN driver for the PIC18Cxx8



A CAN driver for the PIC18Cxx8



A CAN driver for the PIC18Cxx8