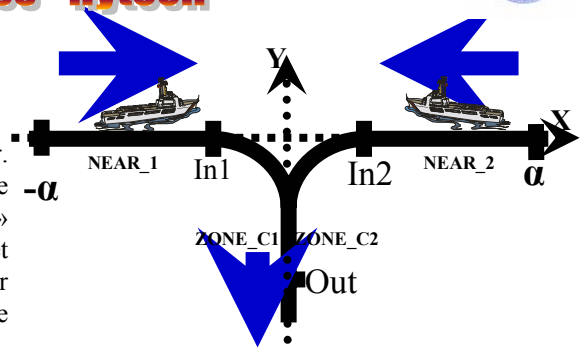
ULB

Faculté des Sciences - Département d'Informatique

Systèmes hybrides - Hytech

Expérience : Contrôle du passage de 2 supertankers dans un canal commun. On ne peut avoir qu'un supertanker dans la zone critique (zone_c1 et zone_c2) pour éviter une collision.

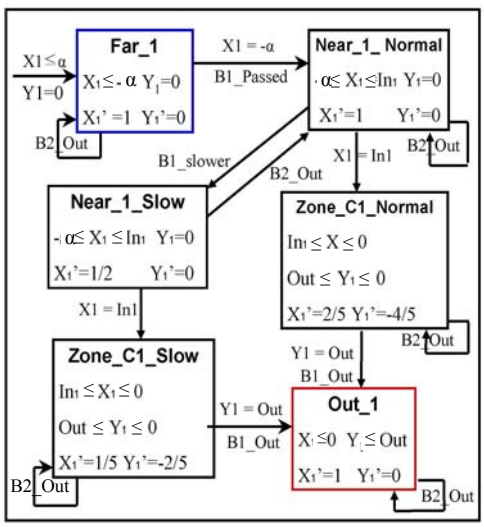


• Le comportement des 2 bateaux est dicté par un contrôleur. Quand un bateau atteint α ou -α, le contrôleur vérifie si l'autre bateau n'est pas déjà dans une des zones «near» ou «zone_c» opposée. Si oui, alors il oblige le deuxième bateau à ralentir et ce dernier retrouve sa vitesse de croisière lorsque le premier bateau arrive à Out. Sinon il continue son chemin à vitesse normale.

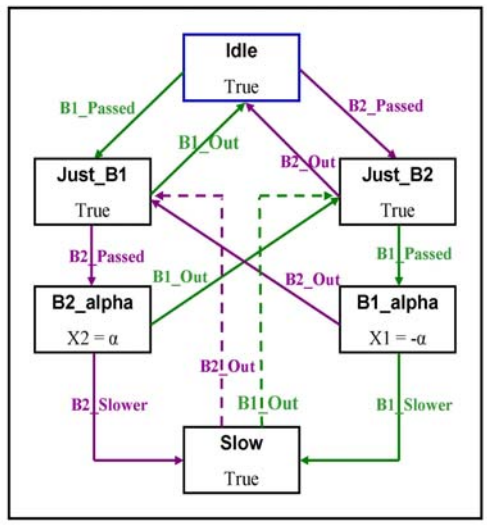
On modélise ce système par une combinaison d'automates hybrides linéaires : un par bateau et un pour le contrôleur.

Modélisation : Système hybride : Sextuple < ***Loc***, ***Var***, ***Lab***, ***Edg***, ***Act***, ***Inv*** >

Automate supertanker 1:



Automate Contrôleur :



Hytech : outil de spécification et de vérification du système hybride.

But : L'état initial du système est <FAR1,FAR2,IDLE>, et l'état final est <OUT1,OUT2,IDLE>. On veut vérifier que l'on peut atteindre l'état final à partir de l'état initial, mais tout en évitant de passer par l'état de collision qui est <Zone_C1_Normal, Zone_C2_Normal, ANY> ou <Zone_C1_Slow,Zone_C2_Slow,ANY> ou ...

Comment : On utilise la méthode «forward analysis» avec Hytech.

On obtient le système hybride final en calculant la composition parallèle des 3 automates hybrides. Sur ce système, on peut définir des régions. Une région est un ensemble (l, P), où l est une location de l 'automate et P est un ensemble de valeurs que peuvent prendre les variables dans cette location.

Ensuite hytech calcule «the forward reachable region» en trouvant la limite de la séquence infinie I, post(I), post²(I), ... des régions, où I est l'état initial et où l'opérateur post(W) est l'ensemble de tous les états successeurs d'une région W via une transition ou un écoulement de temps. Dès lors, «the forward reachable region» est défini comme l'ensemble de tous les états accessibles à partir de l'état W après un nombre fini de transitions,

càd $post^*(W) = \cup_{i\geq 0} post^i(W)$.

Soit C l'état de collision, on veut alors que $post^*(I) \cap C = \varnothing$. Pour chaque région, Hytech nous fournit les conditions sur chaque variable et paramètre permettant d'y être. On connaît donc l'intervalle des valeurs de α pour être dans l'état C. Il suffit donc de prendre un α hors de cet intervalle pour qu'on n'atteigne jamais cet état.

Difficultés : On utilise un outil comme hytech car tous ces calculs sont très lourds, et on peut assister à une augmentation du nombre des régions et de la complexité de celles-ci avec l'accroissement du nombre de variables et de locations de chaque système hybride.