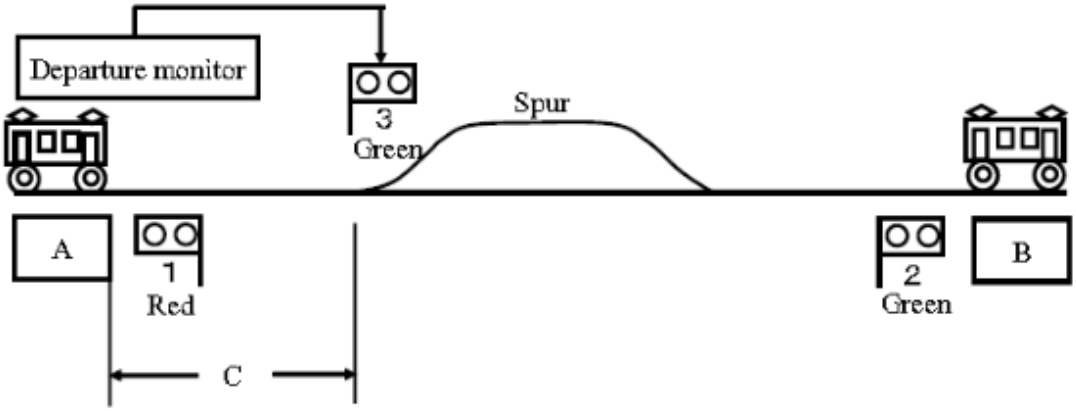
TD n° 2 : Analyse de Risques

Cours «Sûreté de Fonctionnement des Systèmes à Autonomie Décisionnelle »
Année 2020-2021
B. Monsuez

Arbre de défaillance

Exercice 1 : Analyse Préliminaire de Risque



Nous considérons un train avec une voie unique. Nous considérons que le train A part de manière inopiné et franchisse le feu rouge. L'information du départ du train n'a pas été communiquée au terminal B.

Normalement, un système de surveillance détecte les départs inopinés de trains et dans un tel cas de figure met le signal 3 au rouge pour éviter toute entrée dans la section C.

Question 1 : Etablir l'arbre des évènements qui en partant de l'hypothèse d'un départ inopiné du train A pouvant conduire à une collision ou non.

Nous considérons que pour ce faire que le train B n'ayant aucune information contraire considère que la voie est libre.

Nous considérons que le conducteur du train A peut décider de franchir le carré s'il considère que le feu rouge semble bloqué !

Question 1.1 : Etablir la liste des décisions prises par le système. Ces décisions sont soit des détections, sectionnement du système, soit au contraire des actions humaines.

Question 1.2 : En considérant pour chacune de ces décisions une erreur

Pour ce faire, il faudra analyser l'ensemble des positions du train B et l'ensemble des défaillances possibles gérant les différents systèmes.

Question 2 : En considérant pour chacun des évènements que vous avez identifié à la question précédente une probabilité P_i, donné une estimation de la probabilité d'une collision en fonction de la probabilité que chacun de ces évènements se produise.

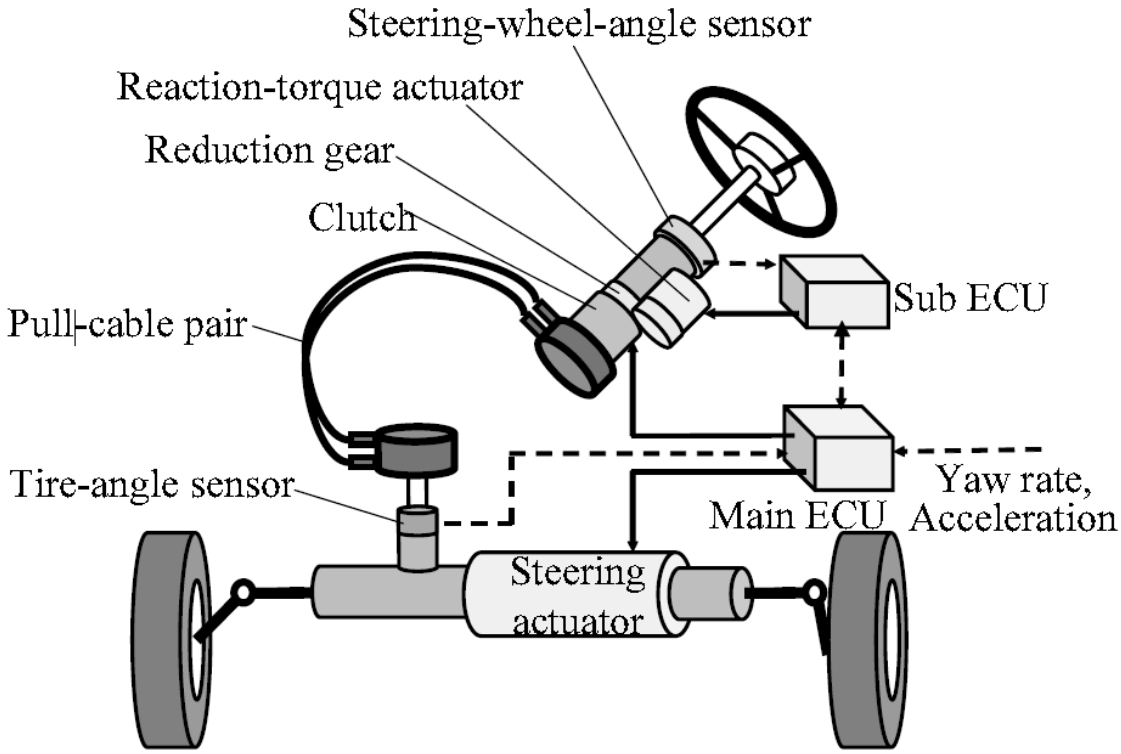
Cette situation s'est produite au japon, le feu rouge était bloqué et le train s'est engagé sur la voie unique. La chaîne de défaillance successive a eu pour conséquence 42 morts.

Une situation équivalente s'est produite il y a quelques mois en Allemagne, conduisant à une dizaine de morts !

Architecture Embarquée Critique

Exercice 2 - Drive-by-Wire

Considérons le système suivant correspondant à un système de direction électronique.



Le calculateur Sub ECU a pour but de piloter le moteur de retour de force.

Le calculateur ECU a pour but de piloter l'actionneur contrôlant la direction.

Question 1 : Effectuer une analyse de l'ensemble des composants électroniques (capteurs, actionneurs, calculateurs) et déterminer les conséquences des défaillances de chacun de ces capteurs.

Question 2 : Classer l'ensemble des défaillances répertoriées par niveau de gravité.

Question 3 : Estimer le niveau de fiabilité de l'architecture en supposant que chaque composant a une probabilité de faute de 10^{-7}.

Question 4 : Proposer une chaîne de calcul Capteur/Calculateur/Actionneur permettant d'atteindre un niveau de fiabilité allant au-delà de 10^{-11}.

Question 5 : Que se passe-t-il en cas de perte de l'alimentation électrique ? Quelles sont les solutions pour pallier cela ?

Question 6 : La commande par câble sert de commande de redondance. Proposer une solution simplifiée que la chaîne de calcul Capteur/Calculateur/Actionneur qui lorsqu'une défaillance est détectée bascule le fonctionnement sur la commande par câble.

Question 7 : Dans le cas de figure suivant, quel est le niveau de fiabilité que doit vérifier la commande par câble pour atteindre un niveau de fiabilité allant au-delà de 10^{-11}.

Question 8 : Nous ne sommes pas intéressées pour l'instant au « Steering Actuator ». Il est important de surveiller son bon fonctionnement. Proposer un mécanisme de surveillance qui s'assure qu'il fonctionne bien et en cas de défaillance bascule sur la commande par câble.