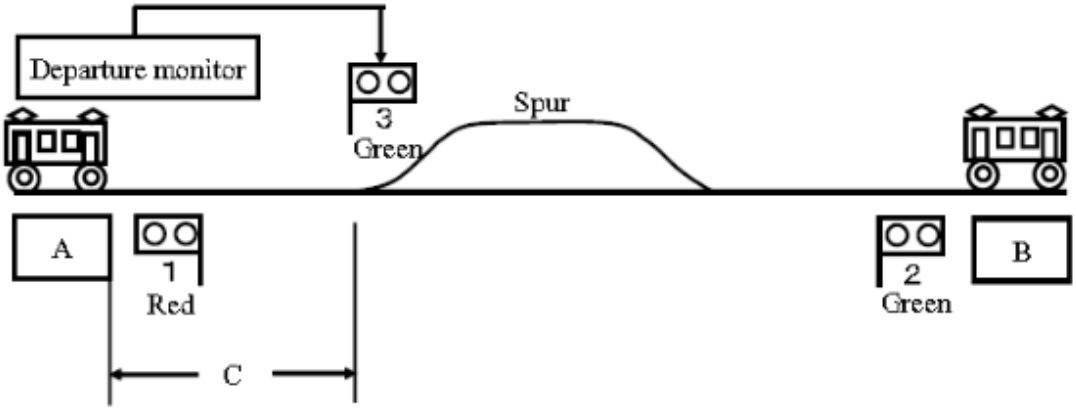
TD n° 2 : Analyse de Risques

Cours «Sûreté de Fonctionnement des Systèmes à Autonomie Décisionnelle »
Année 2019-2020
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.

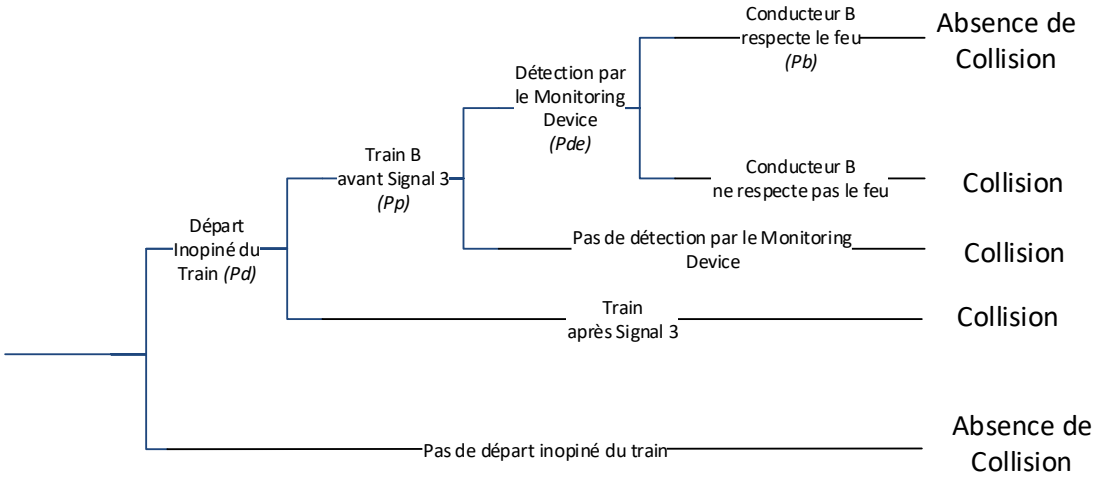
Nous considérons que le conducteur du train A peut décider de franchir le carré s'il considère que le feu rouge semble bloqué !

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.

L'arbre d'évènement suivant répond aux question 1.1 et 1.2 :



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.

La probabilité de collision est par la somme des probabilités de chacun des chemins conduisant à une collision :

$$Pd(1 - Pp) + Pd\ Pp\ (Pde\ (1 - Pb) +\ 1 - Pde)$$

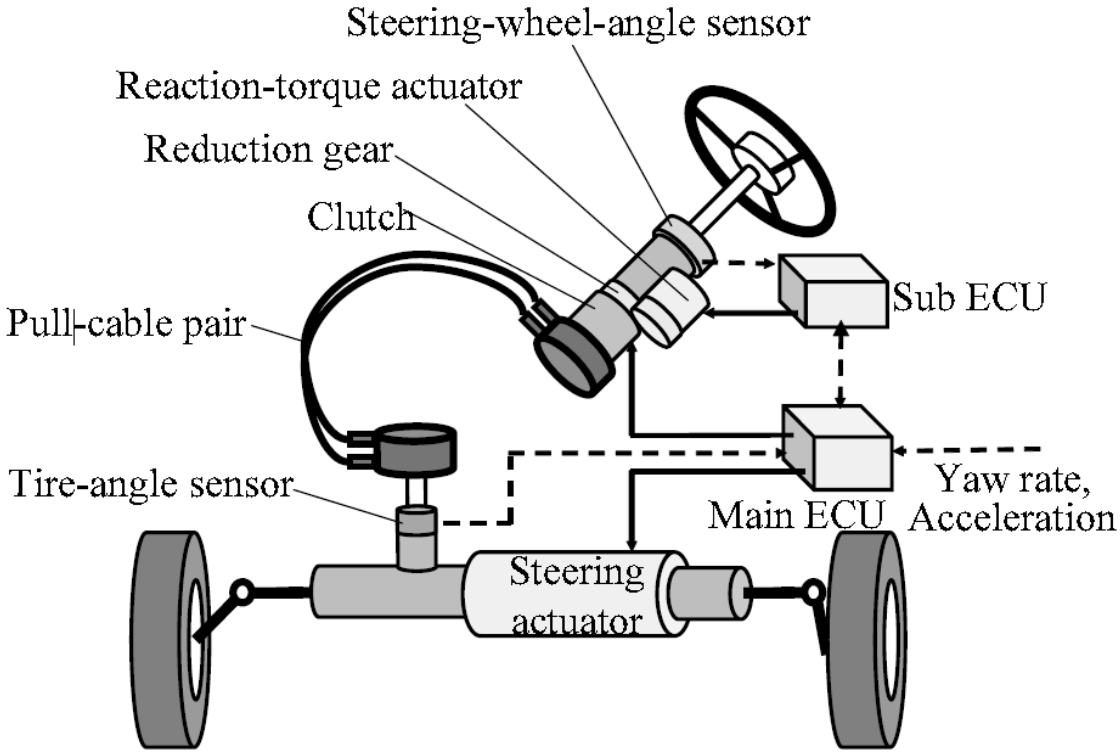
Cette situation s'est produite au japon, le feu rouge était bloqué et le train s'est engagé sur la voie unique. La chaîne de défaillance successive a eu pour conséquence 42 morts.

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.

Evènement redouté : Perte de la Direction

Perte de la commande électrique +

1. Perte du câble de commande
2. Perte de l'embrayage mécanique du câble activée d'une détection de fautes par les deux ECU ne permettant plus la commande électrique, une défaillance totale sur les deux ECUs ou une perte d'alimentation.

Evènement redouté : Perte de la commande électrique

1. Le calculateur principal « MainECU » porte l'intégralité de la commande de l'actionneur. Dans ce contexte, il s'agit d'un équipement dont la défaillance entraine la perte de la commande électrique.
   Nous avons deux calculateur, un calculateur « MainECU », un second calculateur « SubECU », le calculateur principal peut-être redondé par le calculateur secondaire qui supplée le calculateur principal en cas de pertes de la commande.
2. Perte du capteur de volant.
   La perte du capteur de volant entraîne la perte de la commande électrique. La disponibilité pourrait être augmentée en dupliquant le capteur.
3. Perte du capteur d'accélération. La fonction est dégradée en cas de perte, l'assistance n'est plus proportionnelle à la vitesse.
4. Perte de l'actionneur électrique. Une possibilité serait de le dupliquer, cependant, le problème vient du coût de cet équipement.
5. Perte de l'alimentation électrique.

Evènement redouté : Perte du retour d'information dans le volant

1. Perte du capteur de volant.
2. Perte du capteur d'angle au niveau de la crémaillère de direction.
3. Perte du calculateur secondaire « Sub ECU ».
4. Perte du calculateur principal « Main ECU », le calculateur secondaire prenant le relai du calculateur principal.
5. Perte de l'actionneur de retour de force.
6. Perte de l'alimentation électrique.

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

Perte de la Direction : Niveau Catastrophique

Perte de la commande électrique : Niveau Grave (Majeur ?)

Perte du retour d'information dans le volant : Niveau Majeur (Mineur ?)

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

Nous considérons que la **perte de la commande électrique** comme indiqué dans le schéma correspondrait à la perte de l'un quelconque des éléments, donc la probabilité de défaillance serait de l'ordre de 5 10^{-7}.

En fait, certains composants ont malheureusement une probabilité de défaillance bien supérieure, un calculateur est plus proche de 10^{-6} que de 10^{-7}, un capteur plus proche de 10^{-5} que de 10^{-7}. Nous pouvons par contre considérer qu'un actionneur de bonne qualité serait de l'ordre 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}.

Typiquement, l'élément limitant est l'actionneur qui conditionne le niveau de sécurité. En l'absence de redondance, la perte de la commande électrique sera certaine. Nous sommes donc limités à un niveau de fiabilité de 10^{-7} en ce qui concerne la chaîne électrique.

Par contre, pour obtenir ce niveau, nous devons robustifier la chaîne au niveau des capteurs et des calculateurs.

En considérant que les capteurs ont une fiabilité de 10^{-4}, la duplication de capteurs permettrait d'assurer une fiabilité de 10^{-8}. De même, en partant des deux calculateurs, l'un servant de secours au premier, nous pouvons assurer une fiabilité de 10^{-9} pour la chaîne de calcul.

Nous restons cependant assez loin des 10^{-11} qui impliquerait de gérer deux actionneurs et d'ajouter une architecture qui commute d'un actionneur sur l'autre tout en s'assurant que le premier actionneur ne puisse pas influer sur le deuxième actionneur (l'actionneur bloque le comportement du deuxième actionneur).

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

Dans le cas d'une perte de l'alimentation électrique, la perte de la commande électrique est certaine. Le moyen de sécuriser serait de mettre une seconde batterie de secours et un commutateur qui commutera l'alimentation électrique d'une batterie vers l'autre batterie, ce qui permettra d'effectuer de monter à 10^{-10} les risques de perte totale d'alimentation.

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

Cf. Réponse donnée aux questions précédentes.

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}.

Si nous considérons que la fiabilité de la chaîne électrique est de 5 10^{-7} avec un seul actionneur, il est impératif que la chaîne mécanique possède une fiabilité d'au moins 10^{-5} et en prenant une marge de sécurité de 10^{-6} sur ces différents composants que sont les câbles et les embrayages.

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.

Pour ce faire, il faut ajouter un système du type suivant :