Travaux pratiques : Arbres de défaillances pour la modélisation et l'évaluation des systèmes en Sûreté de Fonctionnement*

1. Système de régulation d'un fluide au bord d'un avion

On considère le système de régulation d'un fluide réalisé avec deux vannes proportionnelles montées en redondance (en parallèle) selon le schéma ci-dessous.

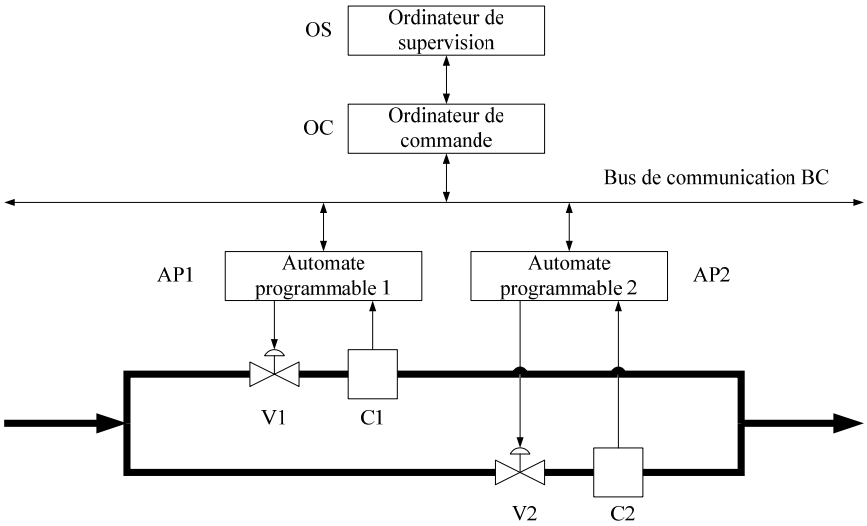


Figure 5. Système de régulation d'un fluide

Chaque vanne V_1 et V_2 est commandée en position par un API différent (AP_1 et AP_2). De plus, on mesure le débit dans chaque dérivation par un capteur (C_1 ou C_2) relié à l'automate correspondant. Les automates sont simplement destinés à commander la position des vannes et à mesurer l'information capteur. Ils transmettent chacun la valeur du débit mesurée à un ordinateur de commande (OC) qui élabore les angles d'ouverture des vannes en fonction des débits mesurés, afin de réaliser des régulations de débit dont les références sont fournies par un ordinateur de supervision (OS). Celui-ci peut demander l'ouverture d'une vanne ou de l'autre ou de deux sachant que chaque vanne est capable de fournir seule le débit maximal de fluide. On suppose que les deux voies sont indépendantes. L'ordinateur de commande dialogue avec les automates à travers un bus de communication (BC). Les automates sont capables d'identifier les défaillances des capteurs et des vannes et de transmettre l'information à l'ordinateur.

On considère les modes de défaillances suivantes :
- défaillance des ordinateurs, du bus, des API et des capteurs
- deux modes de défaillances différents des vannes sont possibles : vannes bloquées fermées ou bloquées non fermées (ouverture quelconque).

1) Etablir l'arbre de défaillances de l'événement **« Régulation de débit impossible sur toute la plage de débit depuis le débit nul jusqu'au débit maximum »**.
   Remarque 1. Pour établir l'arbre de défaillances du système on peut considérer (comme discuté en cours) le paramètre physique qui doit être commandé (le débit) et analyser les différentes situations possibles de ce paramètre.
   Remarque 2 Les automates programmables ayant deux fonctions, chacune de ces fonctions peut être en impossibilité d'être exécutée par l'automate programmable indépendamment de l'autre dû au fait que chacune de fonction utilise une carte différente de l'automate (la fonction de mesure utilise la carte d'entrée, la fonction de commande utilise la carte de sortie), ces cartes pouvant être défaillantes indépendamment l'une de l'autre la fonction de mesure
   Pour des raisons de simplification, on peut considérer que la probabilité de défaillance de chacune de ces fonctions (y compris celle de la carte utilisée) sera égale à la probabilité de défaillance de l'automate qui réalise cette fonction.†

*Vos remarques et commentaires à propos de ce sujet sont les bienvenus. Contact : Nicolae.Brinzei@univ-lorraine.fr
†En réalité dans un automate programmable, il faudrait considérer au moins les composants suivants : une alimentation, une carte qui implémente la logique de décision, une carte d'entrée, une carte de sortie, un bus de communication entre les cartes).

2) Déterminer la probabilité d'occurrence de l'événement redouté (ainsi que des événements intermédiaires) à un an de fonctionnement et tracer son évolution dans le temps. Qu'elle sera la fiabilité de ce système ?
   Tracez la courbe représentant l'évolution de la fiabilité et de la probabilité de défaillance du système dans le temps.
   Au bout de combien de temps la probabilité de défaillance du système devient supérieure à 0.01 ?
3) Déterminer les coupes minimales, ainsi que leurs probabilités. Quelle est la coupe la plus critique ?
4) En analysant ces résultats, comment l'architecture de ce système pourrait être modifiée afin d'améliorer le système ?

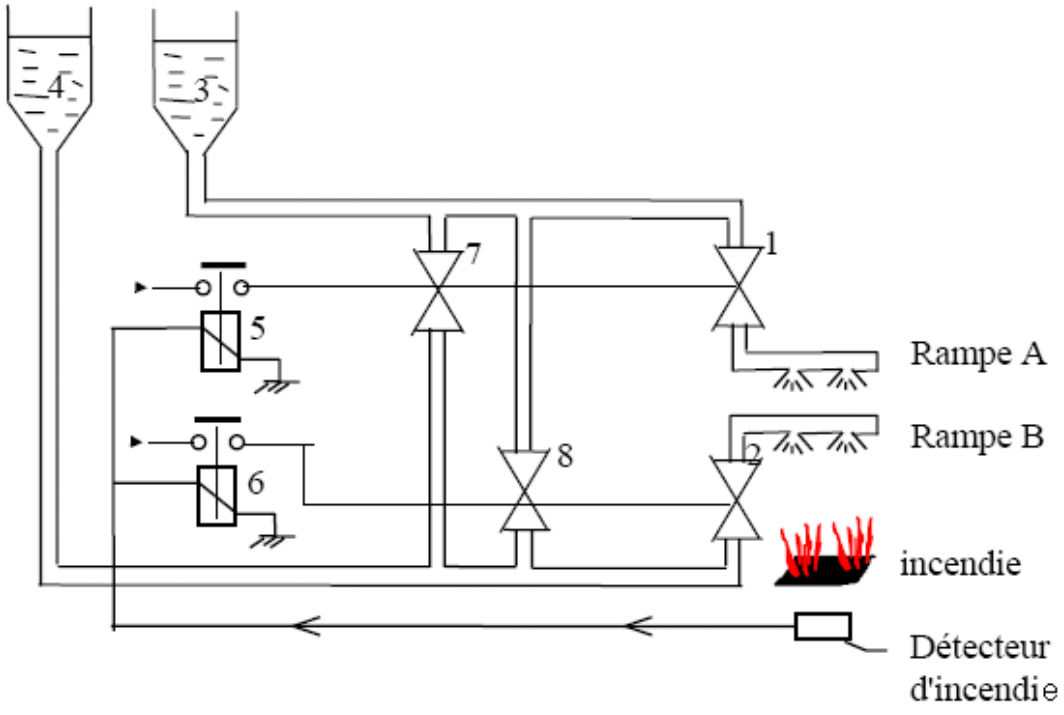
Les défaillances de différents composants suivent des lois de probabilités de taux suivantes : $\lambda_{API} = 3 \cdot 10^{-6}\,h^{-1}$, $\lambda_{ordinateur} = 5 \cdot 10^{-6}\,h^{-1}$, $\lambda_{BC} = 8.5 \cdot 10^{-6}\,h^{-1}$, $\lambda_{capteur} = 10^{-4}\,h^{-1}$.

Les défaillances des vannes (pour chaque mode de défaillance) sont décrites par une loi de Weibull des paramètres suivants :

- paramètre d'échelle $\alpha_{vanne} = 12000\,h$
- paramètre de forme $\beta_{vanne} = 2.5$
- paramètre de localisation $T_0 = 0\,h$.

2. Dispositif d'extinction d'incendie

Lorsqu'un incendie est détecté, deux relais (5 et 6) commandent respectivement l'ouverture de deux vannes (1 et 7, respectivement 2 et 8) de manière à alimenter deux rampes d'arrosage à partir de deux réservoirs (3 et 4). Les défaillances de composants sont considérées comme indépendantes.



Types de défaillance :
- Vannes 1, 2, 7, 8 : non ouverture des électrovannes
- Relais 5, 6 : non action des relais
- Réservoirs 3, 4 : réservoirs vides ou colmatés

1) Etablir l'arbre des défaillances menant à l'évènement redouté *« non extinction de l'incendie par l'une ou l'autre des deux rampes »*.
2) Déterminer la probabilité d'occurrence de cet événement et tracer son évolution dans le temps.
3) Trouver les coupes minimales et leurs probabilités d'occurrence.

4) La défaillance d'une des vannes 7 ou 8, est-elle plus critique que celle d'une des vannes 1 ou 2 ? Justifier votre réponse.
5) Un mode de DCC affecte le groupe des vannes 1 et 7, respectivement 2 et 8. Déterminer la fiabilité de ce groupe des vannes sans ou avec la prise en compte des DCC. Etudier l'effet de la méthode de calcul des DCC[‡]. Déterminer également la fiabilité du système global sans ou avec la prise en compte des DCC.
6) Déterminer le taux de défaillance équivalent du système.

Application numérique :

- réservoirs : $\lambda_{res} = 5 \cdot 10^{-6}$ h
- relais testés périodiquement : $\lambda_{relai} = 2 \cdot 10^{-5}$ h , date du premier test pour le premier relai $T_0 = 1$ an et pour le deuxième relai $T_0 = 2$ ans , période de test pour les deux relais $\tau = 2$ ans [§]
- vannes : $\lambda_{v1} = \lambda_{v2} = 4 \cdot 10^{-6}$ h , $\lambda_{v7} = \lambda_{v8} = 8 \cdot 10^{-6}$ h , $\beta = 10\%$.

[‡] GRIF permet l'utilisation de plusieurs méthodes pour le calcul des DCC : minimum, maximum, moyenne arithmétique, moyenne géométrique (cf. au manuel utilisateur).
[§] Ce comportement peut être modélisé sous GRIF avec une loi TPS « test périodique simple » (voir le manuel utilisateur pour la description détaillée de cette loi).