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

1. Système instrumenté de sécurité pour la protection d'un réservoir

Soit un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil. Ce réservoir peut rejeter des gaz dans l'atmosphère. Une analyse des phénomènes dangereux liés à ce système a montré que les systèmes de protection disponibles (alarmes et niveaux de protection) intégrés au réservoir sont insuffisants pour assurer le risque acceptable (non-dépassement du seuil imposé pour le rejet des gaz). Pour améliorer la protection, un système instrumenté de sécurité (SIS) est proposé par le concepteur du système (voir figure). Ce SIS est composé des capteurs de flux, des capteurs de pression et des capteurs de température. En fonction des informations fournies par ces capteurs, deux unités de traitement LS_1 et LS_2 élaborent les consignes nécessaires à destination des deux électrovannes. Pour élaborer une consigné les unités de traitement doivent disposer de l'information sur les trois paramètres physiques (flux, pression, température) simultanément. Les capteurs de flux sont en logique 2 parmi 3 (2oo3) et les autres composants du SIS sont en logique 1 parmi 2 (1oo2). Les composants du SIS sont connectés à un réseau de communication dont on suppose que sa probabilité de défaillance est négligeable en comparaison avec les autres composants du SIS.

Les taux de défaillance des composants du SIS sont les suivants : $\lambda_{FT} = 10^{-5}\ h^{-1}$, $\lambda_{PT} = 2.5\ 10^{-5}\ h^{-1}$, $\lambda_{TS} = 4\ 10^{-5}\ h^{-1}$, $\lambda_{LS} = 2\ 10^{-6}\ h^{-1}$. Les électrovannes sont sujet à deux types de défaillances : défaillances de la partie électrique de l'électrovanne caractérisées par un taux $\lambda_{\text{solénoïde vanne}} = 2.9\ 10^{-5}\ h^{-1}$ et défaillances du bloc mécanique caractérisées par une loi de Weibull des paramètres suivants : paramètre d'échelle $\alpha_{\text{bloc vanne}} = 25000\ h$ †, paramètre de forme $\beta_{\text{bloc vanne}} = 2.5$ et paramètre de localisation $T_{0\ \text{bloc vanne}} = 0\ h$.

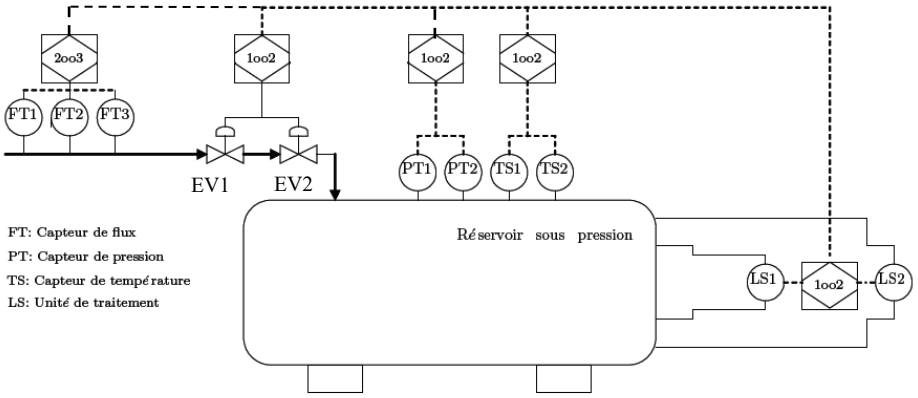

Figure 1. Réservoir sous pression et son SIS

1) Donnez le diagramme de fiabilité du SIS.
   Question supplémentaire : Que deviendrait ce diagramme de fiabilité s'il suffisait que les unités de traitement disposent de la connaissance d'au moins un seul paramètre physique pour être capables de prendre une décision ?
2) Quelle est la fiabilité de ce système à un an de fonctionnement ? Et à 10 ans ?
   Tracez la courbe représentant l'évolution de la fiabilité du SIS dans le temps.
3) Les capteurs de flux sont soumis à un mode de DCC avec un $\beta = 10\%$. Calculez la fiabilité de ce groupe des capteurs en présence de DCC. Comparer sa fiabilité avec celle obtenue dans le cas sans DCC.
4) Déterminez le taux équivalent de défaillance du système.
5) On considère maintenant que le réseau de communication n'est plus supposé exempté de défaillances et son taux de défaillance est de $\lambda_{\text{réseau}} = 10^{-9}\ h^{-1}$. Quelle place prend-il dans le diagramme de fiabilité ? Quelle est la fiabilité du système à un an de fonctionnement ?
6) Le concepteur décide de changer l'architecture du SIS. Ainsi les deux électrovannes ne sont plus en logique 1oo2 et chacune sera commandée par une seule unité de traitement à laquelle l'électrovanne sera affectée (EV_1 sera commandée par LS_1 et EV_2 sera commandée par LS_2). De plus une troisième électrovanne EV_3 sera montée en série avec les deux déjà existantes et elle sera commandée soit par LS_1, soit par LS_2.
   Donnez le diagramme de fiabilité dans ce cas et déterminer la fiabilité équivalente du SIS à un an. Comparez cette nouvelle architecture avec l'architecture standard.

*Vos remarques et commentaires à propos de ce sujet sont les bienvenus. Contact : Nicolae.Brinzei@univ-lorraine.fr

† The scale parameter or characteristic life estimates is the life which corresponds to a cumulative mortality of 63.2% of the population.

2. Système de stockage des données

Un système de stockage des données (figure 2) est constitué de deux unités de stockage en parallèle connectés par un réseau de communication. Chacune de ces unités est constituée de deux disques durs organisés dans une structure spécifique appelée RAID (Redundant Array of Independent Disks).

Le RAID 0 est une version connue sous le nom d'« entrelacement de disques » ou de « volume agrégé par bandes ». Les données à sauvegarder (un fichier par exemple) sont découpées en plusieurs bandes de taille fixée et ces bandes seront réparties successivement sur l'ensemble des disques disponibles. Ainsi, l'écriture (respectivement la lecture) d'un fichier pourra être effectuée simultanément sur chacun des disques durs, ce qui a pour effet de diminuer les temps d'accès (lecture et écriture) aux données. Par conséquent, le RAID 0 augmente les performances et permet d'atteindre un débit de lecture et d'écriture très élevé. La capacité de tous les disques d'une unité de stockage en RAID 0 est également augmentée (n fois la capacité du plus petit disque, où n représente le nombre de disque du RAID 0).

Le RAID 1 est une version qui assure en temps réel une duplication des données sur tous les disques de la structure qui contiennent à tout moment exactement les mêmes données. L'écriture des données se fait de manière simultanée sur tous les disques (ainsi les disques sont interchangeables à tout moment). Ainsi, le débit maximal sera limité par le disque le plus lent. La lecture se fait sur le disque le plus facilement accessible au moment de l'opération. Le RAID 1 est orienté vers la sécurité de données et sa capacité totale est égale à la capacité du plus petit disque dur.

Les deux unités de stockage (RAID 0 et RAID 1) sont connectées en parallèle au réseau de communication et elles sont utilisées pour sauvegarder les mêmes données. Ainsi le système de sauvegarde fonctionne (les données peuvent être stockées ou récupérées par le système d'exploitation tant qu'au moins une unité fonctionne.

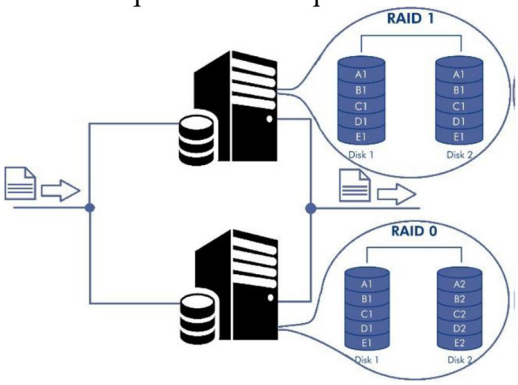

Figure 2. Système de stockage des données

1) Déterminez le diagramme de fiabilité du système de stockage des données.
2) On dispose des quatre disques durs dont leurs caractéristiques sont données dans le tableau 1. Comment affecterez-vous ces disques aux deux unités de stockage ?
3) On considère que la durée de fonctionnement avant défaillance des disques durs est distribuée suivant une loi exponentielle de paramètre $\lambda = 1/MTTF$. Les disques sont caractérisés par un taux de défaillance annualisé (Annualized Failure Rate - AFR) qui est donné par l'équation suivante[‡] :

$$AFR = 1 - e^{-\frac{8766}{MTTF}}$$

Déterminez le taux de défaillance λ de chacun des disques.

Tableau 1. Caractéristiques des disques durs utilisés dans le système de stockage des données[§]

HDD	***Capacité [To]***	***AFR***
SEAGATE ST6000DX000	6	0.0143
WDC WD60EFRX	6	0.0568
SEAGATE ST3000DM001	3	0.2672
HGST HDS5C3030ALA	3	0.0082

‡ H. Lundberg, "Reliability Estimates in Electronics Industry "Reliability study in the HFC network", Turku University of Applied Sciences, 2020. Disponible : https://www.theseus.fi/bitstream/handle/10024/336054/Lundberg_Heidi.pdf?sequence=2.

§ A. Klein, "Backblaze Hard Drive Stats for 2016," 2017. Disponible : https://www.backblaze.com/blog/hard-drive-benchmark-stats-2016/.

4) Calculez et tracez l'évolution dans le temps de la fiabilité de chaque unité de stockage. Analysez les résultats.
   En considérant que les 4 disques sont tous identiques (par exemple de type WDC WD60EFRX) analysez et comparez les deux types de RAID.
5) Calculez et tracez l'évolution dans le temps de la fiabilité et respectivement de la probabilité de défaillance dans le temps. Au bout de combien de temps la fiabilité devient inférieure à 0.99 ?
6) Afin de pallier les défaillances potentielles de disques, on met en place une stratégie d'inspections périodiques des disques, chaque disque étant testé périodiquement tous les 6 mois. Si une défaillance est détectée lors d'un test, alors le disque défaillant est réparé. La réparation est caractérisée par un taux de réparation : $\mu = 2 \cdot 10^{-2}\ h^{-1}$.**
   Quel sera l'impact de cette stratégie sur la fiabilité de chaque unité de stockage et sur la fiabilité du système complet ?
7) Déterminez les coupes minimales du système.
8) Une troisième unité de stockage est rajoutée en parallèle avec les deux premières. Cette nouvelle unité de stockage est constituée des 3 disques WDC WD60EFRX montés en RAID 5.
   Le RAID 5 combine le RAID 0 (méthode du volume agrégé par bandes) à une parité répartie. La parité, qui est incluse avec chaque écriture, se retrouve répartie circulairement sur les différents disques. Chaque bande est donc constituée de n blocs de données et d'un bloc de parité (OU exclusif). Ainsi, en cas de défaillance de l'un des disques, pour chaque bande il manquera soit un bloc de données soit le bloc de parité. Si c'est le bloc de parité, ce n'est pas grave, car aucune donnée ne manque. Si c'est un bloc de données, on peut calculer son contenu à partir des n-1 autres blocs de données et du bloc de parité.
   a) Déterminez le diagramme de fiabilité du système de stockage des données.
   b) Calculez la fiabilité de l'unité RAID 5 et comparez cette méthode avec les méthodes précédentes RAID 0 et RAID 1.
   c) Calculez la fiabilité du système de stockage complet.

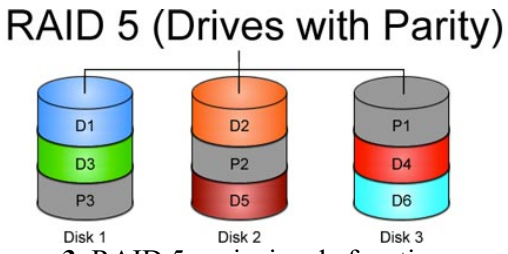

Figure 3. RAID 5 : principe de fonctionnement.

** Ce comportement peut être modélisé sous GRIF avec la loi intitulée « TPE / Tests périodiques étendue » (voir le manuel utilisateur pour la description détaillée de cette loi).