Serious game sur la sécurité fonctionnelle IEC 61508 : Le jeu "SIL Facile"
Serious game on functional safety IEC 61508 : The game "SIL easy"

Laurent Cauffriez
laurent.cauffriez@uphf.fr

Univ. Polytechnique Hauts-de-France, LAMIH, CNRS, UMR 8201, F-59313 Valenciennes, France

RESUME : Le jeu "SIL Facile" sur les niveaux de SIL ─ abréviation anglo-saxonne pour Safety Integrity Level ─ a été proposé dans le cadre d'une pédagogie active en école d'ingénieurs sur la sécurité fonctionnelle et la maîtrise des risques. L'idée de ce serious game est de modéliser le processus de défaillances d'un système instrumenté de sécurité en utilisant un lancer de dé et le tirage de cartes portant des instants de défaillance. Ce jeu a pour objectif d'illustrer les connaissances élémentaires en mathématiques sur les épreuves de Bernoulli, le schéma de Bernoulli, l'espérance d'une variable aléatoire, la probabilité moyenne sur un intervalle de temps. Ces connaissances mathématiques sont nécessaires pour bien assimiler la notion de PFDaverage telle qu'introduite dans la norme de sécurité fonctionnelle IEC61508 dédiée à l'évaluation du niveau de SIL d'architectures de sécurité à base de technologie Electrique, Electronique et Programmable Electronique. Ce jeu a fait l'objet d'un dépôt auprès de l'INPI sous forme d'une enveloppe Soleau.

Mots clés : Jeu pédagogique, Serious game, Niveaux d'intégrité de sécurité, Safety Integrity Level, SIL, Sécurité fonctionnelle, Systèmes E/EP/E, Norme IEC61508, Réduction du risque, Maîtrise des risques.

1 INTRODUCTION

La conception des systèmes instrumentés de sécurité doit répondre à des normes de sécurité fonctionnelle souvent difficiles à comprendre.
L'idée du serious game "SIL Facile" est de modéliser le processus de défaillances d'un système instrumenté de sécurité en utilisant un lancer de dé et le tirage de cartes portant des instants de défaillance.
L'objectif pédagogique est de faciliter la compréhension de la notion de "Probabilité moyenne de défaillance dangereuse PFDaverage" qui s'applique pour l'évaluation du niveau d'intégrité de sécurité (niveaux de SIL) des Systèmes Instrumentés de Sécurité (SIS).
Cette notion de PFDaverage a été introduite dans la norme de sécurité fonctionnelle IEC61508 [1]. Cette norme a été ensuite étendue à d'autres domaines : CEI 61511 pour l'industrie de transformation, CEI 62061 dans le domaine des machines, CEI 61513 pour le nucléaire, ISO 26262 dans l'automobile, EN 50126/128/129 pour le ferroviaire.
Au-delà de son application aux systèmes instrumentés de sécurité, ce jeu peut être utilisé pour enseigner la simulation de Monte Carlo et illustrer la génération de variables aléatoires suivant une loi de distribution, exponentielle dans le cas présent.

2 LA SECURITE FONCTIONNELLE [2]

La sécurité fonctionnelle se définit comme un sous-ensemble de la sécurité globale et s'applique à tous systèmes Electriques, Electroniques, Programmables Electroniques (E/E/PE) concernés par la sécurité.
Un Système Instrumenté de Sécurité (SIS) à base de technologie E/E/PE comprend tous les éléments nécessaires à l'exécution de la fonction de sécurité : alimentation, matériel, logiciel, unités logiques, unités d'entrées et de sorties, transmetteurs, actionneurs, systèmes de communication, actions humaines.

Une fonction de sécurité définit ce qui doit être réalisé pour éviter des situations dangereuses (arrêt d'un moteur en un temps limité) ou pour prévenir le danger (éviter un démarrage intempestif).
Pour chaque fonction de sécurité, il faut préciser la mission de la fonction de sécurité, ce qui doit être surveillé, l'action qu'il faut réaliser lors de l'occurrence d'une défaillance en précisant le temps de réponse imparti, prédire le comportement du système.

Les principaux termes relatifs au domaine de la sécurité fonctionnelle sont rappelés ci-dessous.

Une fonction de sécurité est une fonction devant être implémentée dans un système E/E/PE concerné par la sécurité dans le but d'atteindre ou de maintenir un état sûr de l'équipement sous contrôle (Equipment Under Control) en dépit de l'occurrence d'un événement dangereux particulier.
Un système de sécurité implémente les fonctions de sécurité nécessaires pour atteindre ou maintenir un état sûr de l'équipement contrôlé avec pour objectif d'atteindre, seul ou avec d'autres systèmes E/E/PE, l'intégrité de sécurité requise.
L'intégrité de sécurité vise à garantir qu'un système concerné par la sécurité exécute de manière satisfaisante les fonctions de sécurité dans toutes les conditions spécifiées et dans une période de temps donnée.
Quatre niveaux d'intégrité de sécurité (Safety Integrity Level) sont usuellement assignés aux systèmes de sécurité : le niveau 1 (SIL1) est le plus bas niveau d'intégrité de la sécurité, et le niveau 4 (SIL4) est le niveau d'intégrité de sécurité le plus élevé.
Le défi est de concevoir le système de sécurité de manière à éviter les défaillances dangereuses et à les contrôler lorsqu'elles surviennent. La démarche repose dans un premier temps sur une analyse et une classification du risque. Cette activité peut être réalisée par diverses

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20222017

méthodes quantitatives et/ou qualitatives Analyse Préliminaire des Risques (APR), Analyse des Modes de Défaillances de leurs Effets et de la Criticité (AMDEC), Arbre de défaillances et doit aboutir à une liste de risques dont l'évaluation est quantifiée et mise en regard des objectifs du risque maximal tolérable.
La première difficulté de l'étude est que quelqu'un doit s'engager sur le risque maximal tolérable "Maximal Tolerable Risk" (MTR) à atteindre. En principe, il s'agit de l'utilisateur/exploitant final. Pour ce faire, il doit comparer la probabilité de chaque risque au risque tolérable qu'il s'est lui-même fixé. Cette comparaison conduit à identifier la réduction de risque à obtenir par la mise en œuvre d'une fonction intégrée de sécurité indépendant du système de commande de l'équipement sous-contrôle EUC concerné. A noter que, sans cette valeur de risque maximal tolérable, il n'y a pas d'ingénierie de sécurité possible.
La figure 1 illustre la démarche de réduction du risque telle que donnée dans [3]. L'introduction d'un canal de sécurité composé d'un capteur, d'un actionneur et d'un système PES (Programmable Electronic System) conduit à un facteur de réduction du risque RRF (Risk Reduction Factor) de 100 car on passe d'une fréquence d'accidents de 10^{-3} an^{-1} pour le système à sécuriser (EUC) à un MTR de 10^{-5} an^{-1} pour le système global.

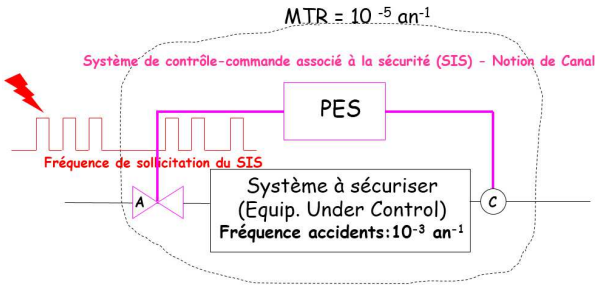

fig 1 : Notion de réduction du risque

L'analyse préalable des risques relatifs à une installation doit prendre en compte :
- la survenue de l'événement indésirable (exprimé soit sous la forme d'un taux d'occurrence soit la forme d'une probabilité) ;
- la conséquence ou sévérité S du risque (notion de gravité) ;
- la fréquence d'exposition F (rare, fréquente ou continue) ;
- la possibilité P d'éviter l'événement (moyens matériels et/ou organisationnels).

Le concept de graphe de risques appliqué en sécurité machine [4] illustre cette démarche de réduction du risque (cf. *fig 2*) :
- S désigne la sévérité de la blessure avec S1 blessure légère normalement réversible, S2 blessure grave normalement irréversible incluant le décès,
- F définit la fréquence et/ou durée d'exposition au phénomène dangereux avec F1 rare à assez fréquente et/ou courte durée d'exposition, F2 fréquente à continue et/ou longue durée d'exposition,
- P donne la possibilité d'éviter le phénomène dangereux ou de limiter le dommage avec une possibilité P1 sous certaines conditions, ou une faible/rare possibilité P2 sans mise en place d'un système de sécurité,
- PL exprime le niveau de performance (Performance Level) requis allant de "a" à "e" et pouvant être traduit en termes de SIL (Safety Integrity Level).

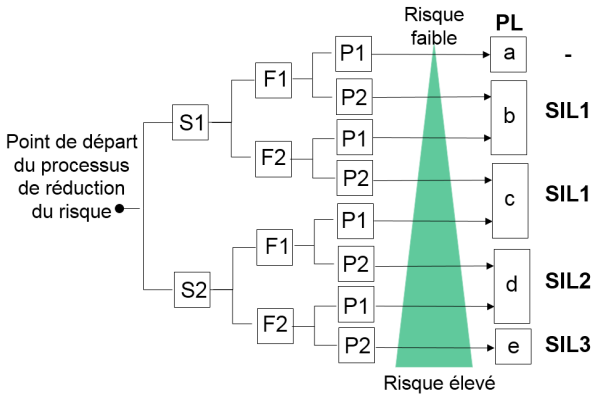

fig 2 : Graphe de risques

La norme considère que l'occurrence d'une défaillance au sein du système de sécurité peut empêcher la fonction de s'exécuter et conduire a fortiori à la perte de la réduction de risque initialement souhaitée.
Pour pallier ce pire cas, des tests appliqués aux composants du système E/E/PE sont réalisés de manière périodique pour s'assurer que la fonction de sécurité soit à même de réaliser sa mission. Si ces tests périodiques conduisent à la détection d'une défaillance au sein du système E/E/PE, le système est réparé et remis dans l'état aussi bon que neuf.
D'un point de vue mathématique, une question à se poser, et sur laquelle il faut sensibiliser les élèves, est l'impact du test périodique sur la fonction de répartition des défaillances.

3 FORMALISATION MATHEMATIQUE DU PROBLEME

3.1 Rappel de fiabilité

La probabilité de défaillance d'un composant à l'âge t est donné par l'équation (1) où :
- T est la variable aléatoire modélisant la durée de vie du composant,
- f(t) est la densité de probabilité.

$$F(t) = P(0 \le T \le t) = P(0 < T < t) = \int_0^t f(t) \cdot dt \qquad (1)$$

La fiabilité est la probabilité de survie à l'âge t, inclusif ou exclusif, elle est donnée par l'équation (2).

$$R(t) = P(T \ge t) = P(T > t) = 1 - P(0 \le T \le t) \qquad (2)$$

3.2 Probabilité de défaillance et de survie d'un SIS 1oo1

En fait, tester périodiquement le système de sécurité et le remettre dans l'état aussi bon que neuf en cas de détection de défaillance conduit à faire travailler le SIS dans une zone de fiabilité réduite à l'intervalle de temps [0, T1], T1 étant l'intervalle de temps entre 2 tests.
Fort de ce constat, il est aisé de quantifier la probabilité de défaillance sur [0,T1] et la fiabilité à l'âge t d'un SIS 1oo1 en appliquant les équations (1) et (2). Il vient les équations (3) et (4) pour une fonction de répartition exponentielle des défaillances càd pour une fonction densité de probabilité égale à $f(t)=\lambda \cdot e^{-\lambda \cdot t}$:

$$F_{1oo1}(t) = 1 - e^{-\lambda \cdot t} \quad \text{définie} \quad \forall t \in [0,T1] \qquad (3)$$

$$R_{1oo1}(t) = e^{-\lambda \cdot t} \quad \text{définie} \quad \forall t \in [0,T1] \qquad (4)$$

A noter que la probabilité maximale de défaillance du SIS sur l'intervalle [0,T1] est donnée par la valeur de t égale à T1 et ne peut en aucun dépasser la valeur Pmax donnée par (5). En effet, le test périodique implique une troncature à droite en T1 de la fonction de répartition, fonction de répartition qui n'est donc pas définie pour un temps t > T1.

$$Pmax = F_{1oo1}(T1) - F_{1oo1}(0) = 1 - e^{-\lambda \cdot T1} \qquad (5)$$

3.3 Notion de Probabilité moyenne de défaillance sur [0,T1] pour un SIS 1oo1

La norme IEC61508 introduit la notion de probabilité moyenne de défaillances dangereuses appelée PFDaverage (Average Probability to Fail Dangerously on Demand) pour des fonctions de sécurité à faible sollicitation [1]. Sa définition est donnée par l'équation (6) pour un SIS 1oo1 où F(t) est la fonction de répartition des défaillances sur l'intervalle [a,b] égal à [0,T1]:

$$\begin{aligned} PFDaverage &= \frac{1}{b-a}\int_a^b F(t)\cdot dt \\ &= \frac{1}{T1-0}\int_0^{T1}(1-e^{-\lambda \cdot t})\cdot dt \end{aligned} \qquad (6)$$

Afin de faire la démarche de réduction du risque donnée figure 2, le concepteur d'un SIS 1oo1 doit calculer le PFDaverage défini par l'équation (6) et confronter la valeur obtenue aux valeurs données dans le Tableau 1 tiré de la norme IEC61508 afin d'identifier le niveau de SIL requis pour la fonction de sécurité envisagée.

Tableau 1. Niveaux d'intégrité de sécurité selon la norme IEC61508 basée sur la probabilité moyenne de défaillance

SIL	PFDaverage
4	$[10^{-5}, 10^{-4}[$
3	$[10^{-4}, 10^{-3}[$
2	$[10^{-3}, 10^{-2}[$
1	$[10^{-2}, 10^{-1}[$

3.4 Points durs mathématiques mis en exergue par le jeu "SIL Facile"

L'objectif principal du jeu pédagogique proposé est d'illustrer la notion de PFDaverage et de démontrer l'impact de la troncature de la fonction de répartition des défaillances sur l'espérance mathématique de la variable aléatoire. Pour mémoire, l'espérance d'une variable aléatoire est calculée à partir de (7).

$$E(T) = \int_0^T t \cdot f(t) \cdot dt \qquad (7)$$

L'équation (8) donne la définition de la densité de probabilité usuellement prise dans les études classiques de fiabilité. Dans ce cas, l'espérance E(T) de la variable aléatoire de distribution exponentielle tend vers la valeur $1/\lambda$ lorsqu'on fait tendre T vers $+\infty$ dans le calcul de l'intégrale donnée par l'équation (7).

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} \ \forall\, t \in [0,+\infty[\qquad (8)$$

L'équation (9) donne l'expression de la densité de probabilité qu'il faut impérativement prendre pour une variable aléatoire de distribution exponentielle tronquée à droite en T1 d'après [5]. L'espérance E(T) de la variable aléatoire tronquée en T1 tend dans ce cas vers la valeur T1/2 conformément à la démonstration faite dans [6] pour un SIS 1oo1 si l'on procède à une linéarisation à l'ordre 2 des termes exponentiels de l'expression donnant E(T).

$$f(t) = \begin{cases} \lambda \cdot e^{-\lambda \cdot t} \cdot \left(1 - e^{-\lambda \cdot T1}\right)^{-1} & \text{si } t \in [0, T1] \\ 0 & \text{sinon} \end{cases} \qquad (9)$$

L'erreur souvent commise par les élèves est de considérer que E(T) tend vers $1/\lambda$ alors que E(T) tend en réalité vers T1/2 pour un SIS 1oo1. A noter que la valeur de $1/\lambda$ est très grande devant T1/2 compte tenu des faibles probabilités données dans le Tableau 1 pour le PFDaverage.

3.5 Proposition de modélisation du processus de défaillance d'un SIS par un schéma de Bernoulli

Pour une période de test iT1 avec i allant de 1 à *n*, le SIS peut :

- Soit faire l'objet d'une défaillance durant l'intervalle de test [i T1, i+1 T1]
- Soit ne pas faire l'objet de défaillance durant l'intervalle de test [i T1, i+1 T1].

Il y a donc deux issues possibles au test périodique :
- soit succès, matérialisant la défaillance du SIS avec une probabilité $p = 1 - e^{-\lambda \cdot T1}$

- soit échec càd le SIS survit à l'âge T1 avec une probabilité $1-p=\mathrm{e}^{-\lambda\cdot \mathrm{T1}}$.

Ceci est la définition même d'une épreuve de Bernoulli puisque le SIS est soumis à *n* épreuves indépendantes conduisant à un schéma de Bernoulli tel que décrit à la figure 3. Pour la première période de test, il y a une probabilité *1-p* que le SIS survive à l'âge T1 (Echec : "Pas de défaillance du SIS") et une probabilité *p* que le SIS défaille sur [0,T1] (Succès "Défaillance du SIS"). Ceci est vrai pour le 2ème test périodique, pour le troisième test périodique, et ainsi de suite jusqu'au *n*-ième test périodique.
Cet enchaînement d'épreuves de Bernoulli à 2 issues mutuellement exclusives conduit à ce qu'on appelle en mathématique un schéma de Bernoulli [7]-[9].

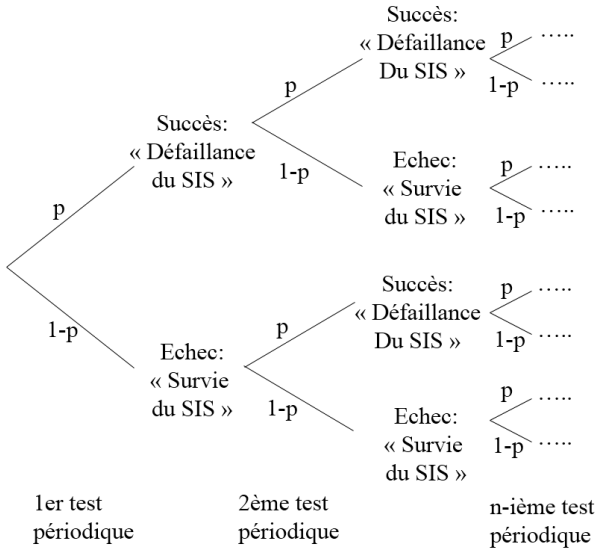

fig 3 : Schéma de Bernoulli pour modéliser le processus de défaillances d'un SIS

Soit X la variable aléatoire représentant le nombre de succès pour une séquence infinie d'expériences de Bernoulli. Soit *n* les *n* premières expériences et *p* la probabilité de succès, on a d'après [9]-[10] que :

- la moyenne du nombre de succès se rapproche d'un nombre appelé espérance de X donnée par l'équation (10)

$$\mathrm{E}(X) = n \cdot p \qquad (10)$$

- l'écart type autour de la moyenne est donnée par l'équation (11)

$$\sigma X = \sqrt{n \cdot p \cdot (1-p)} \qquad (11)$$

- la "cote en faveur d'un succès" càd en faveur de la défaillance du SIS (Odds on favour) est donnée par (12):

$$\mathrm{O}f = \frac{p}{1-p} \qquad (12)$$

- Pour une population très grande d'expériences càd quand $n \to +\infty$, la probabilité que les expériences aboutissent à un succès est donnée par

$$\frac{Expérience\ avec\ succès}{n} \to p \quad \text{lorsque } \mathrm{n} \to +\infty \qquad (13)$$

Pour illustrer cette notion de "Odds on favour of a Success", le tableau 2 donne la valeur d'O*f* pour quelques probabilités de défaillance. A titre d'exemple, pour une probabilité $p=10^{-2}$, la valeur de l'Of=1/99 indique qu'il faut s'attendre à 1 succès contre 99 échecs soit à 1 test périodique pour lequel le SIS fait l'objet d'une défaillance contre 99 tests périodiques sans défaillances.

Tableau 2 : Illustration du concept de "Cote pour un succès"

p	"Cote pour" la défaillance du SIS
10^{-5}	1/99999
10^{-4}	1/9999
10^{-3}	1/999
10^{-2}	1/99
10^{-1}	1/9

L'idée du serious game "SIL Facile" est de modéliser le processus de défaillances d'un système instrumenté de sécurité en utilisant un lancer de dé pour matérialiser la répétition d'épreuves aléatoires indépendantes. En cas de Succès de l'épreuve càd en cas de défaillance du SIS, le tirage d'une carte permet d'obtenir l'instant de défaillance du SIS pour l'épreuve considérée.
Ci-après sont énoncées les règles du jeu de SIL pour un SIS 1oo1.

4 RÈGLES DU SERIOUS GAME "SIL FACILE"

Au préalable, l'enseignant fait un rappel sur la notion d'épreuves de Bernoulli à deux issues mutuellement exclusives (succès ou échec), de schéma de Bernoulli (répétition d'épreuves de Bernoulli indépendantes) et sur le calculant de l'espérance E(X) de la variable aléatoire modélisant le processus de défaillances du système de sécurité étudié.
Le jeu s'applique à tout type d'architectures de sécurité à 1 canal (1 out 1), à 2 canaux (2 out 2), à 1 canal parmi 2 (1 out 2) et 2 parmi 3 (2 out 3) symbolisées communément dans la norme IEC61508 par 1oo1, 2oo2, 1oo2, 2oo3. Dans cette publication, seules sont présentées les règles du jeu pour une architecture 1oo1.
Les cartes portent les instants de défaillances TTF (Time To Failure) exprimés en heures ainsi que la probabilité de défaillances pour l'instant "t" mentionné sur la carte. La fonction de répartition des défaillances est supposée exponentielle.
La version du jeu pour une architecture SIS 1oo1 utilise un dé ainsi qu'un jeu de cartes disposées dans un sabot. On choisit la face "1" du dé pour modéliser la défaillance du SIS ; les faces "2" à "6" modélisant la survie du SIS.
Au début du jeu, un joueur est choisi pour animer le jeu. Le rôle du joueur-animateur est de gérer la succession

des périodes de tests Ti du SIS et de noter sur un document récapitulatif : le nombre total de périodes de tests simulés au cours du jeu, les périodes de test Ti qui ont fait l'objet d'une défaillance, les instants auxquels le SIS a défailli (càd le TTF Time To Failure) pour la période de test considéré ainsi que la probabilité de défaillance du SIS à cet instant mentionnée sur la carte tirée par l'élève.

Le jeu se déroule de la manière suivante :

i) Le joueur-animateur invite le premier joueur à lancer le dé pour simuler la première période de test T1 du SIS.

Si le joueur obtient un "1", le SIS défaille et le joueur tire une carte qui lui donne l'instant auquel le SIS a défailli sur la période de test.

Si le joueur tire une valeur "2 à 6", le SIS survit et le joueur passe la main au joueur suivant après y avoir été invité par le joueur-animateur.

ii) Le joueur suivant lance à son tour le dé pour simuler la deuxième période de test du SIS.

Les mêmes règles que celles données au point i) sont appliquées selon l'issue du lancer de dés. Le jeu se poursuit en enchaînant les périodes de tests sous le contrôle du joueur-animateur jusqu'à ce que toutes les cartes du sabot soient épuisées. Pour une partie plus longue, le joueur-animateur peut remettre les cartes dans le sabot après les avoir mélangées.

iii) En fin de partie, les joueurs dont le joueur-animateur synthétisent les résultats :
- en donnant le nombre total *n* de périodes de tests comptabilisées et simulées à la fin de la partie,
- en précisant le nombre de fois *n1* que le SIS a défailli sur les *n* périodes de tests simulées et comptabilisées,
- en calculant le Mean Time To Failure,
- en calculant la moyenne des probabilités de défaillance du SIS figurant sur les cartes, c'est à dire le PFDaverage,
- en identifiant la cote en faveur d'une défaillance du SIS (Odds on),
- en identifiant la probabilité maximale Pmax atteinte au cours de la partie et le time to failure TTF associé permettant ainsi aux joueurs de déduire les valeurs de T1 et le taux de défaillance λ pour le SIS 1oo1 simulé (identification a posteriori de cette grandeur).

Les joueurs peuvent en outre aisément vérifier que le PFDaverage est donné pour une valeur de *t* tendant vers la valeur T1/2 lorsque la variable aléatoire modélisant le processus de défaillances du SIS suit une loi exponentielle tronquée à droite en T1 (cf. équation (9)) ; ce qui n'est bien sûr pas le cas pour une fonction densité définie sur $[0,+\infty[$ pour laquelle le time to failure TTF tend vers $+\infty$ lorsque la valeur de Pmax tend vers 1 (cf. équation (8)).

5 PRESENTATION DU JEU

Le serious game "SIL Facile" propose 2 jeux de cartes : un jeu avec une fonction de répartition exponentielle des défaillances tronquée à droite en T1 et définie pour $t\in[0, T1]$, et un jeu avec une fonction de répartition exponentielle définie pour $t\in[0, +\infty[$. Selon le temps disponible et l'effectif total du groupe d'élèves, l'enseignant peut enchaîner les parties avec chacun des jeux de cartes proposés ou scinder le groupe d'élèves en deux, chaque groupe jouant une partie avec le jeu de cartes qu'il lui a été attribué. Cette deuxième manière de faire oblige à désigner deux joueurs-animateurs parmi les élèves et présente l'avantage de confronter les résultats obtenus par chacun des groupes. Elle permet aux élèves de bien comprendre l'impact de la troncature de la fonction de répartition des défaillances sur le calcul du PFDaverage et du Mean Time to Failure. L'analyse faite à la fin de la partie leur permet d'identifier la modélisation la plus fidèle du processus de défaillances d'un SIS en la confrontant aux expressions théoriques données dans la norme IEC61508.
La figure 4 donne un descriptif du jeu "SIL facile". On y distingue la piste de dés, le sabot de distribution des cartes, et les 2 jeux de carte portant les instants de défaillances du SIS. Les cartes sont "typées" par des versos différents et portent la mention "Université polytechnique" et "INSA Hauts-de-France" selon que le jeu de cartes correspond à une fonction de répartition tronquée ou non.

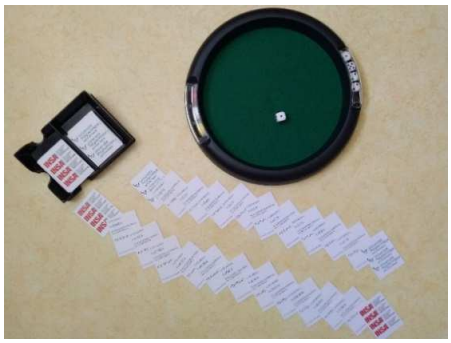

fig 4 : Descriptif du jeu "SIL Facile"

La figure 5 présente un exemple de carte telle que manipulée par les élèves. On y retrouve l'instant *t* auquel le SIS défaille ainsi que la probabilité de défaillance du SIS à l'âge *t* porté par la carte, probabilité de défaillance qui est égale à F(t)-F(0)=F(t) par application des équations (1) et (3). En fin de partie, les élèves peuvent facilement vérifier si la moyenne des instants de défaillance tend soit vers T1/2 (loi tronquée) soit vers $1/\lambda$ (loi complète) et ainsi rattacher le jeu de cartes au cas d'étude qu'il leur a été attribué. A noter que le cas d'étude n'est pas communiqué aux élèves par l'enseignant en début de partie car il appartient aux élèves de faire la synthèse et tirer les conclusions au vu des données stochastiques manipulées durant le déroulé du jeu.

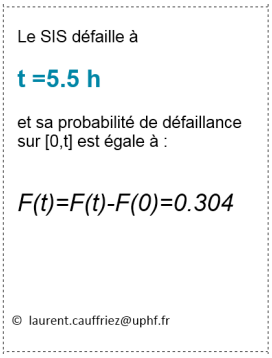

fig 5 : Exemple de carte manipulée par les élèves

6 RETOUR D'EXPERIENCE SUR LE SERIOUS GAME "SIL FACILE"

J'ai mis en place le jeu "SIL Facile" dans mes enseignements à l'INSA Hauts de France, récemment créée à Valenciennes, fort du constat que les élèves éprouvaient certaines difficultés à la maîtrise des "savoirs" dans le domaine des probabilités lorsqu'elles sont appliquées en ingénierie. En gestation depuis deux ans et créé initialement sous Excel avec une démonstration interactive en cours magistral par vidéoprojecteur, j'ai finalement décidé d'opter pour un jeu alliant un dé et des cartes pour une pédagogie active de style APP (Apprentissage Par Problème) où l'élève est mis dans une situation qui lui permette de construire ses connaissances grâce aux interactions avec les autres ; l'apprentissage résultant du processus de compréhension et de résolution d'un problème : l'identification du niveau de SIL d'un système intégré de sécurité dans le cas présent.

J'ai pu constater que cette pédagogie par le jeu permettait aux élèves de mieux assimiler les notions d'espérance mathématique et de loi de répartition des temps de bon fonctionnement et des temps de défaillances, notions utilisées en sûreté de fonctionnement et en sécurité des systèmes. Calculer une intégrale pour obtenir une valeur de PFDaverage est peu parlant pour les élèves mais générer des défaillances de manière aléatoire, à partir d'un dé et d'un jeu de cartes, pour simuler le processus de défaillances d'un SIS permet aux élèves de mieux cerner cette notion de probabilité moyenne de défaillance. Ce jeu s'avère en outre être un excellent complément pour l'enseignement de modèles stochastiques à base de simulation de Monte Carlo. Les logiciels industriels utilisés en enseignement sont très souvent des boîtes noires et j'ai pu constater que les élèves comprennent difficilement comment sont générées des variables aléatoires à partir d'une fonction de répartition quelle qu'elle soit. Sur ce point, il suffit de demander aux élèves ce que retourne, par exemple, la fonction EXPO(Mean) dans leur modèle de sûreté de fonctionnement ou de simulation de flux pour être convaincu qu'ils ne font pas le lien entre les cours de mathématiques sur les variables aléatoires et les fonctions mises à leur disposition dans les librairies des progiciels industriels du marché.

7 CONCLUSION

L'objectif de cette communication est de présenter le serious game sur les niveaux de SIL Safety Integrity Level que j'ai développé et mis en place en école d'ingénieurs. Ce jeu pédagogique a fait l'objet d'un dépôt auprès de l'INPI sous forme d'une enveloppe SOLEAU. Après une brève introduction, le contexte pédagogique qu'est l'enseignement de la sécurité fonctionnelle de systèmes E/E/PE pour la maîtrise des risques a été décrit. La problématique de la modélisation du processus de défaillances d'un système instrumenté de sécurité périodiquement testé a ensuite été défini mathématiquement. L'apport du jeu a été montré pour une modélisation du processus de défaillances d'un système instrumenté de sécurité s'appuyant sur la notion d'épreuves de Bernoulli, de schéma de Bernoulli, d'espérance d'une variable aléatoire, de probabilité moyenne sur un intervalle de temps. Les règles du serious game "SIL Facile" pour un système intégré de sécurité de type 1oo1 ont ensuite été introduites. Enfin, un retour d'expériences sur l'utilisation de ce jeu avec un public d'élèves en école d'ingénieurs a été donné pour une pédagogie active et une meilleure maîtrise des variables aléatoires utilisées en sûreté/sécurité des systèmes.

Bibliographie

[1] IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems E/E/PE", *Partie 2, Int. Electrotechnical Commission, (2010).*

[2] Cauffriez L., "Polycopié de cours magistral en Sécurité fonctionnelle et Maîtrise des risques", *INSA Hauts de France, Valenciennes (France), 2019.*

[3] Cauffriez L., "A review of SIL theory and a demonstration on the need to truncate the exponential distribution for the generation of SIS failures: Example for a 1oo1 channel architecture", QUALITA, Nancy (France), Mars 2015.

[4] NF EN ISO 13849-1, "Sécurité des machines - Parties des systèmes de commande relatives à la sécurité", *Partie 1, Principes généraux conception, Norme ISO, (2015).*

[5] Al-Athari F.M., "Estimation of the mean of truncated exponential distribution", *Journal of Mathematics and Statistics, 4 (4):284-288, 2008, ISSN 1549-3644.*

[6] Zhang, T., W. Long, and Y. Sato, "Availability of systems with self-diagnostic components applying Markov model to IEC61508-6", *Reliability Engineering & System Safety 80, 133–141, (2003).*

[7] Alston, C.-L., K.-L. Mengersen, A.-N. Pettitt, "Case Studies in Bayesian Statistical Modelling and Analysis", *Wiley Series in Probability and Statistics. J. Wiley & Sons, (2013).*

[8] Hsu H., "Theory and Problems of probability, random variables and random processes", *Schaum's Outline, (1997).*

[9] Cauffriez, L., "Modelling of Safety Instrumented Systems by using Bernoulli trials: towards the notion of odds on for SIS failures analysis", *Journal of Physics: Conference Series, 783 012057. (2017).*

[10] Walsh J.-B, "Knowing the Odds: An Introduction to Probability", *American Mathematical Society 139*, *(2012).*

[11] Cauffriez L. "Review of Mathematical Inconsistencies in the Practices to Assess SIL of SIS: Toward a Novel Approach for Risk Reduction", *ESREL, 22-26 Septembre 2019, Hannovre, Allemagne, (2019).*