1. Introduction

Dans l'industrie, on parle de plus en plus de sûreté de fonctionnement. Cette discipline, qui a acquis ce nom et sa forme actuelle principalement au cours du dernier demi-siècle et dans les secteurs de la défense, de l'aéronautique, de l'espace, du nucléaire, puis des télécommunications et des transports, serait désormais utile, voire indispensable, à tous les secteurs de l'industrie et surtout en environnement.

La sûreté de fonctionnement est une riche palette de méthodes et de concepts au service de la maîtrise des risques.

La sûreté de fonctionnement n'est pas un but en soi, mais un moyen ou un ensemble de moyens : des démarches, des méthodes, des outils et un vocabulaire.

Le but qui impose le recours à la sûreté de fonctionnement est plus reconnaissable sous le terme de « maîtrise des risques ».

La sûreté de fonctionnement (SdF) est d'abord un état d'esprit avant d'être un ensemble de méthodes.

Dans ce cours en va voir les concepts de SdF et quelques méthodes les plus utiliser en domaine de l'environnement. Les exemples d'application seront traités au niveau des séances de TD.

2 Historiques

Selon A. Leroy et J.P. Signoret [1], l'entre-deux-guerres voit émerger les concepts de fiabilité et de taux de défaillance dans l'aéronautique suite à la comparaison des fréquences des pannes des avions bimoteurs et quadrimoteurs et au calcul de ratios, nombre de pannes/nombre d'heures de vol.

À partir de la deuxième guerre mondiale, une discipline se développe sous le nom de « **théorie de la fiabilité** ». Les décennies 1940 et 1950 sont caractérisées par la découverte de l'efficacité d'une approche probabiliste appliquée à l'électronique dans l'aéronautique, la défense et le nucléaire. La formulation de ce qui nous paraît évident aujourd'hui – la probabilité de succès d'une chaîne de composants est le produit des probabilités de succès de chacun des composants – fut l'origine d'un développement très rapide dans les domaines cités.

Cette période fut aussi celle d'un développement rapide de l'électronique qui introduit des composants nombreux dont les défaillances individuelles sont imprévisibles à ce stade des connaissances, mais dont les défaillances collectives présentent des régularités statistiques ; sur un lot de composants homogène, on sait prédire avec une bonne confiance le nombre de défaillances par unité de temps qui vont se produire alors qu'on reste totalement incapable de prédire quel composant va tomber en panne et quand.

À partir de la **décennie 1980**, les efforts entrepris dans tant de directions s'approfondissent, mais aussi tendent à se rejoindre pour constituer cette discipline d'application très étendue qu'est aujourd'hui la **sûreté de fonctionnement**. On note les développements suivants :

- constitution de bases de données de fiabilité ;
- début de normalisation en matière de sûreté de fonctionnement ;
- développement des méthodes d'analyse, de modélisation, de représentation des systèmes complexes ;
- développement de logiciels de calculs ;
- développement de logiciels de modélisation ;
- campagnes d'essais pour recueillir des données de fiabilité ;
- utilisation large ou ciblée de la sûreté de fonctionnement dans la plupart des industries ;
- utilisation de la sûreté de fonctionnement pour maîtriser tout type de risque industriel (et peu à peu des risques juridiques, individuels, financiers, etc.) et non seulement la sécurité ;
- apparition et développement des clauses contractuelles de sûreté de fonctionnement et des exigences légales et réglementaires de sûreté de fonctionnement ; besoin croissant de connaissances pointues dans les domaines scientifiques concernés dans les systèmes complexes : systèmes programmés, sciences humaines et sociales.

  Aujourd'hui, le terme « **sûreté de fonctionnement** » recouvre l'ensemble des moyens qui permettent de se donner et de transmettre une confiance justifiée dans le succès d'un projet, d'une activité et son innocuité.

3. Notions fondamentales

La démarche, le raisonnement « sûreté de fonctionnement » s'appuient sur quelques notions de base qui se sont précisées au cours de son évolution et qui continuent à s'affiner [1].

3.1 Sûreté de fonctionnement

Aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données. On notera que ce concept peut englober la fiabilité, la disponibilité, la maintenabilité, la sécurité, la durabilité... ou des combinaisons de ces aptitudes. Au sens large, la SdF est considérée comme la science des défaillances et des pannes [2].
La sûreté de fonctionnement est souvent définie comme :
— fiabilité, disponibilité, maintenabilité et sécurité ;
— science des défaillances ;
— maintien de la qualité dans le temps.
Toutes ces définitions sont reconnues à divers titres par l'Institut de Sûreté de Fonctionnement (ISDF). Chacune de ces définitions est porteuse de beaucoup du contenu de la SdF, mais chacune est cependant réductrice, trop étroite.
_ La définition « **fiabilité, maintenabilité, disponibilité et sécurité** » fait donc référence aux définitions de ces termes et met en avant la cohérence de ces approches. Par contre, si la fiabilité (ou la maintenabilité, la disponibilité et la sécurité) est aussi une performance d'un système, la SdF ne se réduit pas facilement à une performance.
_ La définition « **science des défaillances** » met l'accent sur la prise en compte des défaillances, de leurs causes, de leurs effets et souligne, en parlant de science, l'importance de

la connaissance sur les défaillances (causes, effets, mécanismes...) sans laquelle il n'y a pas d'approche SdF. Mais elle est réductrice en ce sens que la SdF prend en compte et traite plus que des défaillances. En ce qui concerne les événements finaux (les **conséquences**), la SdF ne prend pas en compte que les défaillances dans l'accomplissement des fonctions requises (ce qui serait seulement une approche fiabilité, maintenabilité, disponibilité ou « dependability »), mais aussi des événements sans rapport avec le cahier des charges fonctionnel du système (approche orientée sécurité). En ce qui concerne les événements initiateurs (les **causes**), la SdF ne se limite pas aux défaillances, mais peut permettre de prendre en compte aussi bien des agressions de l'environnement, des actions inattendues ou interdites des utilisateurs ou des tiers, des phénomènes aléatoires...

_ La définition « **maintien de la qualité dans le temps** » souligne l'importance de la durée et l'importance de la référence à des exigences (explicites ou non). Elle a le défaut de laisser supposer qu'une activité SdF se conduit nécessairement dans le cadre d'une démarche qualité, ce qui est faux. C'est le choix – explicable historiquement – de certains secteurs industriels où la sûreté de fonctionnement est très développée à l'intérieur de l'organisation Qualité, mais n'est pas une nécessité ; d'autres secteurs ont une forte expérience de la sûreté de fonctionnement antérieure à la Qualité au sens moderne incarné par les normes ISO 9 000 et bien d'autres, en particulier une expérience de la sûreté de fonctionnement orientée vers la sécurité. **:** La recherche de termes équivalents dans d'autres langues pose de sérieux problèmes [3]

3.2 Risque

Événement redouté évalué en termes de **fréquence** et de **gravité**. En sûreté de fonctionnement, il s'agit d'identifier les événements indésirables, d'évaluer la fréquence de leurs survenues et de quoi elle dépend, d'évaluer la gravité de leurs survenues et de quoi elle dépend ; de prendre ses décisions en fonction de leurs impacts sur le triplet « événement, fréquence, gravité » qu'on appelle risque.

Reformuler en terme de risque les éléments de décision qui relèvent de la prise en compte des dysfonctionnements, des aléas, des erreurs, des agressions de l'extérieur... c'est déjà intégrer l'esprit de la sûreté de fonctionnement.

Événement redouté ou l'événement incertain, mais comme on n'applique généralement la démarche qu'aux **événements craints**, on a pris l'habitude de parler d'**événement redouté**.

Il faut bien situer la **frontière** entre ce qui peut produire l'événement redouté (c'est-à-dire ce qui pourrait être modifié pour influer sur la survenue de l'événement) et ce sur quoi peut agir l'événement redouté (c'est-à-dire ce qui pourrait être modifié pour influer sur les conséquences de l'événement redouté).

3.2.1 Fréquence C'est l'inverse d'un temps, un nombre d'occurrences par unité de temps. Derrière cette apparente simplicité se cache une notion pleine de difficultés.

_ Le temps en question peut s'exprimer en heures, jours ou années. Encore faut-il préciser si ce sont des jours de calendrier ou des jours ouvrables, des heures sous tension électrique ou des heures de fonctionnement, etc. Le temps peut aussi s'exprimer en nombre de sollicitations, en distance parcourue, en cycles de température, en tonnes supportées, etc. Dans une **démarche d'évaluation des risques**, le choix de l'unité est imposé par le modèle qui décrit le plus fidèlement le comportement du système étudié et qui donne la plus grande confiance dans l'extrapolation de l'avenir à partir du passé.

3.2.2 Gravité

La gravité est la valeur accordée à l'événement. Il est plus parlant, puisque l'on parle d'événements redoutés, de dire « le prix que l'on est prêt à mettre pour éviter l'événement ». Il faut tout de suite remarquer que la gravité est une ***grandeur subjective***. Elle dépend de l'événement, mais tout autant du point de vue duquel on l'évalue.

3.3 Évaluation du risque

Pour l'évaluation du risque il faut avoir des informations claires sur :
— le système auquel on s'intéresse ;
— les mesures du temps qui sont pertinentes pour représenter le système et pour les décisions à prendre ;
— les points de vue de ceux pour lesquels on produit une évaluation.

Quand la fréquence et la gravité s'expriment en chiffres, il est usuel de faire le produit des deux (qu'on appelle souvent **criticité**, mais ce terme connaît diverses acceptions). On considère alors implicitement que deux risques évalués par la même valeur de ce produit sont également acceptables. Il faut toutefois être conscient que cette décision est une décision stratégique lourde et non le simple bon sens.

La façon d'exprimer le risque est de placer chaque événement redouté étudié sur un plan dans un repère dont les axes sont la fréquence f et la gravité g. On peut représenter n'importe quel choix d'équivalence de risques en traçant des lignes qui joignent l'ensemble des points qu'on considère également acceptables. Par exemple, l'hypothèse à propos de la criticité revient à prendre pour lignes isorisques les hyperboles.

Parmi les lignes isorisques, une est particulièrement intéressante : celle qui relie les points à la frontière entre l'acceptable et l'inacceptable. Son tracé, sa forme, est l'expression très lisible des critères d'acceptation des risques. Un risque placé au-dessus d'elle doit être réduit pour devenir acceptable :

– soit on en réduit la fréquence, c'est faire de la ***prévention*** ;

– soit on en réduit la gravité, c'est faire de la ***protection***.

Ce **diagramme fréquence-gravité**, aussi appelé diagramme **de Farmer** (figure **1**), est la façon la plus pratique d'illustrer et de communiquer sur le risque, ses trois composantes, ses deux dimensions...

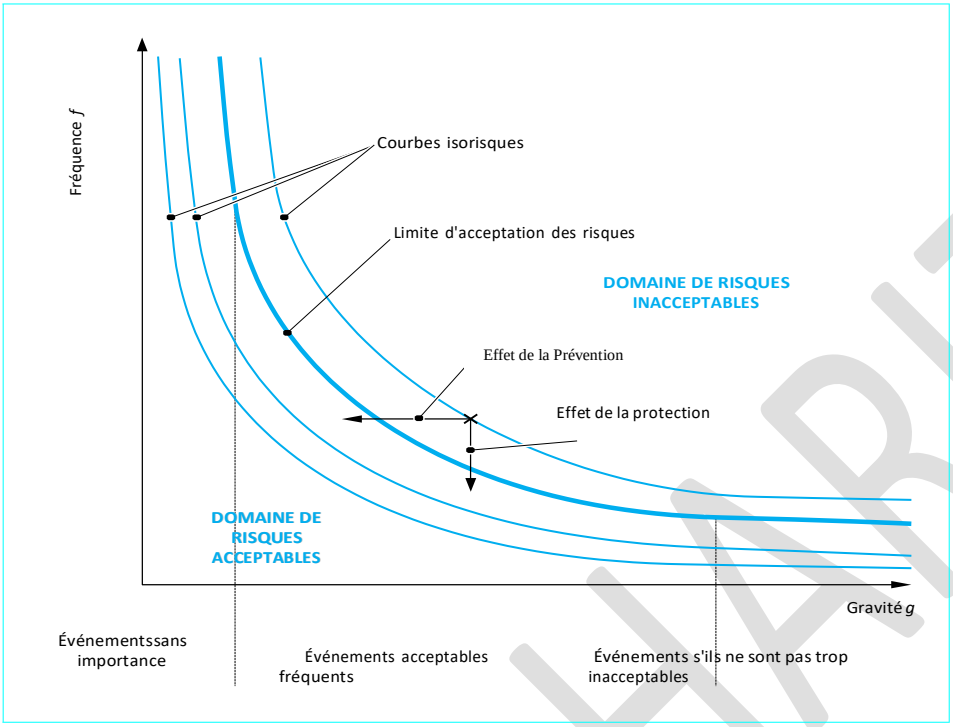

Figure 1 – Diagramme de Farmer [1]

4. Caractéristique de l'SdF

4.1 Fiabilité

Aptitude d'une entité à accomplir les fonctions requises dans des conditions données pendant une durée donnée.

Elle est caractérisée par la probabilité $R(t)$ ou $F(t)$ que l'entité accomplissant ces fonctions à l'instant 0 les accomplisse toujours à l'instant t.

La fiabilité est la notion dont la formalisation et l'approfondisse- ment au milieu du siècle fondent une spécialité (la fiabilité ou le calcul de fiabilité et les fiabilistes qui la pratiquent) qui va s'étendre et rejoindre d'autres approches.

La lettre R est utilisée souvent pour noter la mesure de la fiabilité parce qu'en anglais Fiabilité se dit *Reliability*.

4.2. Maintenabilité

Aptitude d'une entité à être remise en état, par une maintenance donnée, d'accomplir des fonctions requises dans les conditions données.

Elle se caractérise par la probabilité $M(t)$ d'être en état, à l'instant t, d'accomplir ces fonctions sachant qu'elle était en panne à l'instant 0.

La maintenabilité ne se différencie de la fiabilité que sur ce dernier point : elle caractérise la promptitude de reprise du service attendu après interruption. La maintenabilité, c'est la brièveté des pannes (état dû à une défaillance).

4.3. Disponibilité

Aptitude d'une entité à être en état d'accomplir les fonctions requises dans les conditions données.

Elle se caractérise par la probabilité $A(t)$ ou $D(t)$ d'être en état, à l'instant t, d'accomplir les fonctions requises.

La lettre *A* est l'initiale du terme anglo-américain *Availability*.

La disponibilité est une synthèse de la fiabilité et de la maintenabilité ; c'est la proportion du temps passé en état de remplir les fonctions requises dans les conditions données.

L'indisponibilité (son complément) est la proportion du temps passé en panne.

4.4 Sécurité

Aptitude d'une entité à ne pas causer de dommages dans des conditions données ou à ne pas faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Particularités de la sécurité : les éléments communs qui restent généralement liés à l'idée de sécurité sont :

– les événements redoutés sont graves, très graves ;

– la sécurité, c'est de la confiance justifiée (elle ne peut se réduire à un chiffre).

Puisque l'on envisage les événements les plus graves, on envi- sage des risques qui ne sont acceptables que si la fréquence est extrêmement basse. Cela a plusieurs **conséquences** :

– on recherche toutes les possibilités d'accidents graves sans pouvoir négliger ceux qui ont une vraisemblance de se produire très faible ;

– on cherche à évaluer des couples (fréquence-gravité) avec des valeurs infiniment petite/infiniment grande dont la multiplication n'a guère de sens et qui sont extrêmement sensibles aux incertitudes ;

– la détermination de seuils d'acceptation du risque est une démarche difficile et lourde de sens en soi.

Le **taux de défaillance**, généralement noté $\lambda(t)$, est :

$$\lambda(t) = \frac{-dR(t)/dt}{R(t)}$$

Il représente l'intensité de défaillance en fonction du temps. C'est la probabilité conditionnelle, divisée par d*t*, de tomber en panne entre *t* et *t* + d*t* sachant qu'au temps *t* l'entité n'est pas défaillante.

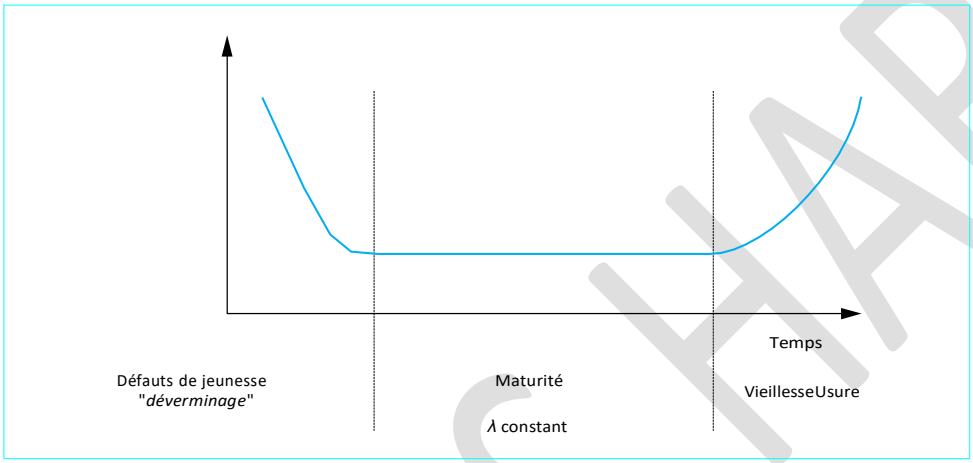

Figure 2 – Taux de défaillance d'une série de composants : courbeen baignoire

L'hypothèse est très souvent faite que ce taux de défaillance est constant (indépendant du temps). Alors la loi de fiabilité prend une forme facile à manipuler de :

$$R(t) = Exp(-\lambda)$$

En fait, cette hypothèse très pratique est assez audacieuse, mais l'expérience a montré que, pour de nombreuses catégories de composants, il y avait une période assez longue entre la jeunesse et la vieillesse pendant laquelle cette hypothèse était une approximation tout à fait acceptable (encore faut-il vérifier qu'on exploitera effectivement cette seule période de la vie des composants si on a pris cette hypothèse pour les calculs prévisionnels).

On constate souvent que la courbe représentant le taux de défaillance d'une série de composants, en fonction du temps à la forme dite « **courbe en baignoire** » (figure **2**) :

– la décroissance rapide de la fréquence des défaillances correspond au « déverminage » et à l'élimination des défauts de jeunesse ;

– le fond de la baignoire correspond à la période de maturité où le taux de fiabilité des composants est le meilleur et, souvent, à peu près constant ;
– enfin, la remontée progressive de la fréquence des défaillances correspond à la vieillesse.

5. Méthodes et outils de l'SdF

Une analyse prévisionnelle de sûreté de fonctionnement est un processus d'étude d'un système réel de façon a produire un modèle abstrait du système relatif a une caractéristique de sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité, sécurité). Les éléments de ce modèle seront des événements susceptibles de se produire dans le système et son environnement, tels par exemple :

{Des défaillances et des pannes des composants du système,
{Des événements lies a l'environnement,
{Des erreurs humaines en phase d'exploitation.
Le modèle permet ainsi de représenter toutes les défaillances et les pannes des composants du système qui compromettent une des caractéristiques de SdF.
An d'aider l'analyste, plusieurs méthodes d'analyse ont été mises au point. Les principales sont :

- APD Analyse Préliminaire des Dangers,
- AMDEC Analyse des Modes de Défaillances et de leurs Effets, et de leurs Criticité
- MDS Méthode du Diagramme de Succès,
- MTV Méthode de la Table de Vérité,
- MAC Méthode de l'Arbre des Causes,
- MCPR Méthode des Combinaisons de Pannes Résumées,
- MACQ Méthode de l'Arbre des Conséquences,
- MDCC Méthode du Diagramme Causes-Conséquences

Dans ce cours on va prendre en étude les deux méthodes les plus utiliser en domaine de l'environnement l'APR et l'AMDEC

5.1. Analyse préliminaire de risques (APR)

Cette **démarche** a pour but de produire une liste d'événements redoutés qui doivent être étudiés. Elle cherche, d'une part, à faire un tour aussi complet que possible des événements redoutés (accidents ou défaillances) et, d'autre part, à écarter rapidement ceux qui ne pourraient conduire à des conséquences assez importantes pour justifier les études. C'est un concept très lâche.

On a l'habitude de la qualifier de « ***méthode de SdF*** ». Dans le sens où méthode évoque des règles, un ordre, une procédure normée reproductible, l'APR en est très éloignée. Elle prend des formes très différentes selon les pratiques : cela va d'un court tableau très synthétique, bâti en une heure ou deux à la lumière de listes types, à une étude très complète et assez détaillée des risques qui concernent un système, en passant par tous les intermédiaires imaginables.

Elle est un peu à elle seule un **résumé d'une démarche de maîtrise des risques** par la SdF :

– identification des événements redoutés, mais sans entrer dans les détails ;

– évaluation et acceptation des risques : il s'agit de retirer de la liste les événements qui sont, *a priori*, sans doute clairement en dessous du seuil à partir duquel ils méritent attention, évaluation aussi précise que possible et arbitrage ;

– maîtrise : mesures propres à réduire et contenir les risques aux niveaux acceptables

Objectifs de l'APR :

– l'identification des événements redoutés (souvent limités à ce qui concerne la sécurité, généralement dans toutes les phases de vie du système) ;

– une évaluation permettant une hiérarchisation de ces risques ;

– l'identification des dispositions de réduction de risques qu'il faudra prévoir (donc spécifier, évaluer en termes de SdF en particulier).

Elle est particulièrement importante dans un projet de système complexe réunissant plusieurs partenaires ayant un rôle significatif dans la sécurité. Elle doit permettre, grâce à la vision globale des risques qu'elle offre, une vision commune à tous ces partenaires des risques, des besoins de réduction de risques, des rôles et responsabilités de chacun.

Cette démarche APR, ou APD (analyse préliminaire de danger) dans certains domaines avec quelques différences, est généralement une première étape indispensable quand des questions de sécurité sont posées. Elle l'est beaucoup moins s'il n'est question que de *F, M, D*. Quand elle est réalisée dès le début, elle sert aussi de référence tout au long du projet.

La **clef** d'une démarche APR est la liste (dans la tête des experts ou dans des documents *ad hoc*) des éléments qui peuvent se réunir pour provoquer un accident : entités dangereuses et situations dangereuses.

5.2 Analyse des modes de défaillance,de leurs effets et de leurs criticités(AMDEC)

C'est la méthode la plus citée au point d'être parfois confondue avec la sûreté de fonctionnement. Le principe de l' AMDEC est le suivant :

– décomposer le système en éléments bien connus ; le niveau de détail de la décomposition se détermine sur ce critère : le niveau auquel on sait associer des modes de défaillance et des fréquences si possible ;

– associer à chaque élément ses modes de défaillance ; chaque mode de défaillance est une façon dont il se comporte à part son comportement prescrit ;

– identifier les effets sur le système de chaque mode de défaillance de chaque élément ;

– éventuellement (c'est cette étape qui distingue l'AMDEC de l'AMDE, Analyse des modes de défaillance et de leurs effets), associer à chacun des modes de défaillance de chaque élément sa criticité, en fonction des effets qu'il produit.

Bien entendu, cette analyse cause/conséquence n'a d'intérêt que si l'on en tire des conclusions. Aussi, les diverses normes officielles, ou de fait, sur l'AMDEC comprennent-elles des suites relatives à l'exploitation de cette analyse qui sont un peu différentes selon le cadre dans lequel la méthode est utilisée

La figure **3** donne un extrait d'un tableau d'AMDEC.

ANALYSE DES MODES DE DÉFAILLANCE, DE LEURS EFFETS ET DE LEUR CRITICITÉ (AMDEC)										
Origine : Pièce :			AMDEC : Produit/Projet NUMÉRO :				Analyste :		Date :	
FONCTIONS (ET/OU) PROCESSUS	DÉFAILLANCE				GRAVITÉ	FRÉQUENCE	DÉTECTION			
	MODE	CAUSE	EFFET	DÉTECTION				ACTION	Responsable	Délai

Figure **3 :** modèle d'un tableau d'AMDEC [4]

Remarque : Quelques exemples d'application sont présentés dans les séances de TD

Références

[1] VILLEMEUR (A.). – *Sûreté de fonctionnement des systèmes industriels*. Éd. Eyrolles, Collection de la Direction des Études et Recherches d'Électricité de France, nº 67, éd. 1997.

[2] Ouvrage collectif ISdF. – *L'état de l'art dans le domaine de la fiabilité humaine*. Éd. Octarès. 1994.

Publications de l'Institut de Sûreté deFonctionnement (ISdF)

[3] Rapport *Les APR appliquées aux transports terrestres guidés*.

[4] Plaquette AMDEC.