TP N° 42

AMDEC et analyses dysfonctionnelles

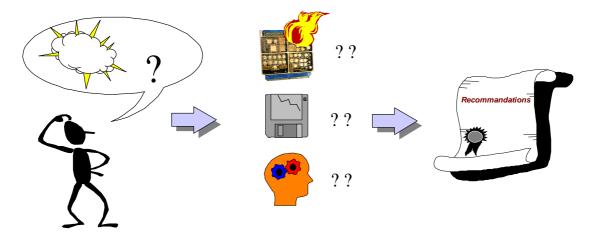
L'objet de ce TP est de rappeler les démarches méthodologiques employées dans l'AMDEC et les analyses dysfonctionnelles afin d'en cerner les apports et limitations pour identifier les risques d'un système. Il est illustré par deux exemples didactiques particulièrement simples.

- 1 Présenter les principales démarches méthodologiques employées pour identifier des risques en soulignant leurs apports et limitations.
- 2 Faire l'analyse des risques d'un frein de vélo
- 3 Faire l'analyse des risques d'un ensemble de liaisons numériques série

1 - Démarches d'identification des risques

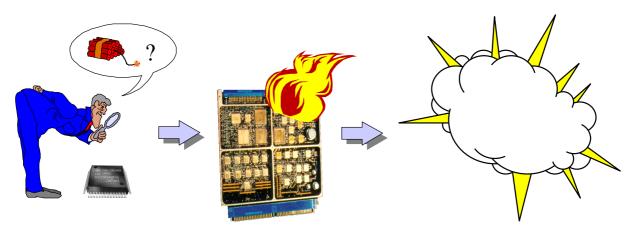
La maîtrise des risques résulte d'une démarche itérative consistant à rechercher et identifier les risques d'un système, les hiérarchiser suivant leur gravité et/ou probabilité d'occurrence puis les accepter ou les traiter par des actions de prévention (pour en diminuer la probabilité) ou de protection (pour en diminuer la gravité).

Outre l'évaluation des marges de dimensionnement qui assurent une certaine robustesse à la conception (analyse pires cas, analyse des contraintes, etc.), les risques peuvent être identifiés par l'exploitation du retour d'expérience (portant notamment sur l'analyse des dysfonctionnements passés) et par deux démarches complémentaires : l'analyse déductive descendante et l'analyse inductive montante.



Analyse déductive descendante

Basé sur l'imagination de l'analyste, la première consiste à identifier à partir d'événements redoutés du système des causes possibles de défaillance de toute nature (matérielle, logicielle, humaine, etc.).



Analyse inductive montante

La seconde consiste analyser les effets au niveau équipement puis sous-système et système de défaillances des composants élémentaires.

L'analyse inductive montante est la principale démarche suivie au cours de l'Analyse des Modes de Défaillance, de leurs Effets et Criticités (AMDEC), notamment quand les modes de défaillance élémentaires à prendre en compte sont connus ou imposés par des normes. Le terme d'AMDEC peut toutefois recouvrir indifféremment les deux démarches, notamment sous la dénomination d'AMDEC fonctionnelle. Le logiciel Failcab emploie les termes d'AMDEC et d'APR (Analyse Préliminaire des Risques) pour différencier les deux démarches.

1.1 – Analyse déductive descendante

Un grand nombre de risques est impossible à imaginer en considérant le système dans son ensemble. Aussi le décompose-t-on préalablement en parties plus facile à appréhender, selon différents aspects tels que fonctionnel, temporel, processus, tâches, etc.

Dans le cas d'une décomposition fonctionnelle arborescente, menée indifféremment jusqu'au niveau adéquat, les risques peuvent être identifiés en s'interrogeant sur l'éventualité de la perte, de la dégradation ou du fonctionnement intempestif de chacune des fonctions élémentaires. Parmi les dégradations envisagées, on considère notamment les perturbations de l'environnement (pollution, dissipation thermique, etc.) ainsi que les sensibilités particulières vis-à-vis de ce dernier.

Dans le cas d'une décomposition temporelle, l'interrogation porte sur l'absence d'événement prévu ou l'apparition possible de séquences erronées.

L'identification de risques conduit à des recommandations diverses telles que :

- Exigences nouvelles concernant les fonctions, les opérations, le matériel, le logiciel (tolérance à une ou plusieurs pannes, robustesse vis-à-vis de l'environnement, etc.),
- Modifications du design telles que la mise en place d'une protection spécifique, d'une redondance locale, d'un observable particulier,
- Procédures opératoires à respecter,
- Formations particulières à dispenser aux opérateurs,
- Demandes d'analyse plus poussée sur certaines composantes (AMDEC, Analyse Pire Cas),
- Etc.

Ce type de démarche présente certains avantages :

- Analyse précoce ayant un véritable impact sur la conception
- Prise en compte de toutes les composantes du système et de leurs interactions
- Ciblage de l'effort nécessaire sur les points identifiés comme critiques
- Mémorisation de la raison de choix techniques

Mais également certaines limitations :

- Difficultés contractuelles pour chiffrer a priori le volume des analyses
- Absence de normes reconnues sur le sujet
- Implication nécessaire de spécialistes dans les divers domaines
- Frein culturel chez certains fiabilistes qui doivent participer à la conception et ne plus se contenter d'une simple action de vérification a posteriori

La démarche déductive est également utilisée dans l'arbre de fautes pour identifier les combinaisons d'événements entraînant la réalisation d'un événement indésirable.

1.2 – Analyse inductive montante.

L'AMDEC se présente sous forme de tableaux à plusieurs colonnes selon les projets et les différentes variantes (AMD, AMDE, AMDEC).

Numéro	Composant	Mode de défaillance	Effets au niveau équipement	Effets au niveau système	Probabilité	Gravité	Symptômes observables	Actions correctives	Observations

Les modes de pannes considérés peuvent être définis au niveau composant ou bloc fonctionnel (quelques composants assurant une fonction élémentaire) et sont généralement issus de normes ou de bases de données.

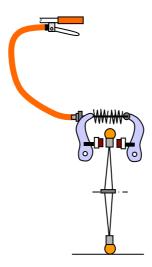
Ce type de démarche présente certains avantages :

- Analyse de l'ensemble des composants d'un produit (\neq exhaustivit\u00e9 des risques identifi\u00e9s)
- Bien adaptée à l'étude des circuits électroniques à base de composants discrets
- Objet de normes diverses (NF X 60-510, CEI 812, MIL-STD-1629A...)
- Permet de trier pour un même symptôme observable l'ensemble des causes possibles, afin de réaliser le manuel de traitement des anomalies utilisé en maintenance

Mais également certaines limitations :

- Analyse mono panne ne prenant pas en compte les défaillances multiples
- Modes de pannes mal ou pas considérés : dérive des paramètres de composants, pannes de composants très intégrés ou à effets non déterministes (ASIC, μP...), anomalies aux interfaces (mécanique), etc.
- Erreurs de conception, de réalisation (logiciel, montage, ...) et d'opérations mal couvertes
- Analyse tardive s'appuyant sur une définition détaillée ayant peu d'impacts réels sur la conception
- Coût prohibitif (bien que prédictible) si généralisée à un système complexe

2 – Analyse des risques d'un frein de vélo



Le frein de vélo est un système mécanique dont les dysfonctionnements résultent essentiellement des interactions entre ses différents composants et non pas de défaillance élémentaire de chacun d'entre eux.

Basée sur une décomposition fonctionnelle, la démarche d'analyse déductive descendante apparaît donc la plus pertinente.

Le frein de vélo peut, par exemple, se décomposer selon l'arborescente suivante afin d'identifier les risques au niveau de chacune des fonctions élémentaires (réalisée au moyen de l'outil APR du logiciel FAILCAB) :

Arborescence

- 1. Frein
- 1.1. Commande de frein
- 1.1.1. Levier (poignée)
- 1.1.2. Rotation de la poignée par rapport au guidon
- 1.1.3. Liaison câble / levier
- 1.2. Transmission de l'effort (câble)
- 1.2.1. Réglage tension câble
- 1.2.1. Embout de gaine
- 1.2.2. Gaine / câble
- 1.3. Freinage
- 1.3.1. Liaison câble / étrier
- 1.3.2. Rotation étrier / cadre
- 1.3.3. Transmission et amplification d'effort (étrier)
- 1.3.4. Rappel par ressort
- 1.3.4. Frottement roue (patin)

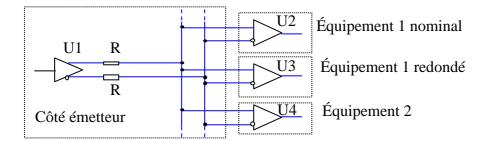
Arborescence	Risques	Gravité	Observations
1. Frein			
1.1. Commande de frein			
1.1.1. Levier (poignée)	Rupture		
	Déformation		
1.1.2. Rotation de la poignée par rapport au guidon	Grippage		
	Perte de l'axe		
	Jeu anormal		
1.1.3. Liaison câble / levier	Rupture liaison		
1.2. Transmission de l'effort (câble)			
1.2.1. Réglage tension câble	Défaut de la		
	Tension câble		
1.2.1. Embout de gaine	Perte étanchéité		graissage
1.2.2. Gaine / câble	Rupture		
	Corrosion / grippage		
1.3. Freinage			
1.3.1. Liaison câble / étrier	Rupture liaison		
1.3.2. Rotation étrier / cadre	Grippage		
	Perte de l'axe		
	Jeu anormal		
1.3.3. Transmission et amplification d'effort (étrier)	Rupture		
	Déformation		
1.3.4. Rappel par ressort	Rupture		
	Force de rappel		
	insuffisante		
1.3.4. Frottement roue (patin)	Arrachement patin		
	Usure importante		
	Blocage intempestif		

3 – Analyse de risques d'un ensemble de liaisons numériques série

Cette fonction est assurée par des composants électroniques dont on connaît les modes de défaillance. La démarche de l'AMDEC classique apparaît donc bien adaptée.

Portant sur une liaison entre un équipement émetteur et 3 équipements récepteurs (dont 2 redondés), l'extrait d'AMDEC suivant se limite aux 3 modes de défaillance suivant de l'un des récepteurs :

- Circuit ouvert
- Court circuit
- Surtension injectée sur la ligne (panne du convertisseur d'alimentation du récepteur)



Liaison numérique RS422

Composant	Modes de défaillance	Effets	Criticité	Recommandations
U2	Circuit Ouvert	Perte de l'équipement 1N Redondance possible (1R)	3	
U2	Court Circuit	Perte de l'équipement 1N Ecroulement du bus Perte mission	1	Placer des résistances de limitation (en série sur les lignes) au niveau des récepteurs
U2	Surtension (alim U2)	Perte de l'équipement 1N Perte du bus Perte mission	1	Protection de l'émetteur et des autres récepteurs / surtension max possible. Pouvoir déconnecter 1N
U3				

Criticité : 1 = Perte Mission, 2 = Mission dégradée, 3 = Mineur