

Note d'application – AMMAR Firas

# Analyse FMEDA dans un Système de Protection d'Onduleur pour Véhicules Électriques

Remplacement de logique de protection discrète par des « Programmable Mixed-Signal Products »



## Étudiants :

Firas AMMAR

Adam-Musharraf IMTHADULLA

## Clients :

M. German HULGICH

M. Victorien AUBRET

## Tuteur industriel :

M. Pascal FICKINGER

## Tuteur de revue :

M. Julian LAURENCE

## Tuteurs académiques :

M. Alexis LANDRAULT

M. Michel JAMES

## Enseignante d'EEO :

Mme. Véronique

QUANQUIN RUET

## Table des matières

1. Introduction.....	3
2. Contexte du projet.....	3
3. Les FSR : Functional Safety Requirements.....	3
4. Types de Fautes et Concepts de FMEDA .....	3
4.1 Types de fautes dans FMEDA .....	4
4.2 Mesures Clés dans FMEDA .....	4
4.3 Normes et Niveaux d'ASIL .....	4
5. Méthodologie pour Analyser les FSR.....	4
6. Analyse de FSR_1 : Détection rapide des surtensions.....	5
6.1 Les mode de défaillance .....	5
6.2 Calcul des FIT pour FSR_1 en se basant sur l'exemple du document Renesas .....	6
6.3 Exemple détaillé pour nOV (broche GPIO) : .....	7
6.4 Mécanismes de sécurité implémentés.....	7
6.5 Conclusion .....	7
7. Analyses des FSR_2 et FSR_4.....	7
8. Analyse de FSR_3 : Détection et déclenchement multiples .....	8
9. Conclusion de la FMEDA.....	9
10. WEBOGRAPHIE .....	10

## 1. Introduction

Dans le cadre de la transition vers des véhicules électriques, la sécurité fonctionnelle des systèmes critiques, tels que les onduleurs, est essentielle. Ces systèmes, qui convertissent l'énergie de la batterie en courant alternatif pour alimenter le moteur, doivent fonctionner de manière fiable. Une défaillance non détectée pourrait entraîner des risques graves pour les passagers et le véhicule.

L'analyse FMEDA (Failure Modes, Effects, and Diagnostic Analysis) permet de détecter, évaluer et atténuer les défaillances potentielles des composants critiques du système. Cette note présente la méthodologie adoptée pour l'analyse FMEDA, les résultats obtenus et leur impact sur la sécurité fonctionnelle du système de protection de l'onduleur.

## 2. Contexte du projet

Ce projet vise à développer une solution programmable pour remplacer un système de protection basé sur une technologie TTL vieillissante. L'objectif est de concevoir un onduleur destiné aux véhicules électriques, intégrant des mécanismes de protection robustes et rapides, permettant de répondre à des exigences de sécurité strictes.

Les principales exigences du projet incluent :

- Respect de la norme ISO 26262, visant à atteindre un niveau ASIL-C ou supérieur.
- Identification des modes de défaillance critiques et conception de mécanismes de diagnostic adaptés.
- Assurer une détection rapide des fautes et une réponse en temps réel.

L'analyse FMEDA est une étape clé pour garantir la conformité de la solution et la sécurité optimale du système.

## 3. Les FSR : Functional Safety Requirements

Les FSR définissent les exigences de sécurité à respecter pour garantir un niveau adéquat de sécurité dans un système critique. Quatre FSR principaux ont été identifiés pour assurer la protection de l'onduleur :

- FSR\_01 et FSR\_02 concernent des délais critiques pour la gestion des états de sécurité (ASC ou FW). Le respect de ces délais est essentiel pour prévenir des défaillances potentielles.
- FSR\_03 implique la gestion des fautes multiples pour activer correctement les sorties (LS-ASC ou HS-ASC).
- FSR\_04 met en évidence l'importance de la cohérence logicielle dans la gestion des signaux de sécurité.

## 4. Types de Fautes et Concepts de FMEDA

## 4.1 Types de fautes dans FMEDA

Dans l'analyse FMEDA, les fautes sont classées selon leur impact sur le système et leur détectabilité. Les principaux types de fautes analysés sont :

- Single Point Faults (SPF) : Défaillances isolées entraînant directement une violation de l'objectif de sécurité sans mécanisme de protection.  
Exemple : Un comparateur qui ne déclenche pas l'état ASC lors d'une surtension.
- Latent Faults (LF) : Des défaillances non détectées qui persistent dans le système et peuvent se combiner avec d'autres fautes pour provoquer un danger.  
Exemple : Une résistance flottante non détectée.
- Residual Faults (RF) : Fautes qui subsistent malgré les mécanismes de sécurité existants, souvent dues à une détection tardive.  
Exemple : Une faute détectée trop tard pour respecter un délai critique.
- Multiple Point Faults (MPF) : Combinaisons de défaillances échappant à la capacité des mécanismes de sécurité pour garantir la sécurité.  
Exemple : Un dysfonctionnement simultané de plusieurs composants critiques.

## 4.2 Mesures Clés dans FMEDA

- SPFM (*Single Point Fault Metric*) : Pourcentage de fautes détectées avant qu'elles ne causent un danger.
- LFM (*Latent Fault Metric*) : Pourcentage de fautes latentes couvertes par des mécanismes de détection.
- PMHF (*Probabilistic Metric for Hardware Failures*) : Mesure des défaillances matérielles par heure de fonctionnement.

## 4.3 Normes et Niveaux d'ASIL

Conformément à la norme **ISO 26262**, les niveaux d'intégrité de sécurité automobile (ASIL A à D) sont définis ou ASIL A : Niveau minimal pour des fonctions critiques et ASIL D : Niveau maximal pour des fonctions vitales, nécessitant des marges de sécurité robustes.

Dans ce projet, les FSR visent principalement ASIL C(D) pour les exigences critiques et ASIL A pour les aspects de cohérence.

## 5. Méthodologie pour Analyser les FSR

Pour chaque FSR, un processus structuré a été suivi :

1. Définition des composants impliqués : Identification des éléments critiques contribuant à l'exigence.
2. Identification des modes de défaillance : Étude de chaque composant pour déterminer ses failles possibles.
3. Évaluation des effets : Analyse de l'impact des défaillances sur le système global.
4. Implémentation des mécanismes de sécurité : Développement des mécanismes pour réduire les risques.
5. Calcul des métriques : Vérification de la conformité aux exigences ASIL en utilisant les SPFM, LFM et PMHF.

## 6. Analyse de FSR\_1 : Détection rapide des surtensions

La première exigence de sécurité fonctionnelle (FSR\_1) stipule que le circuit doit activer la protection ASC (*Active Short Circuit*) dans un délai maximum de 10  $\mu$ s après la détection d'une surtension. Cette réponse rapide est essentielle pour protéger les composants critiques de l'onduleur contre des dommages permanents dus à un dépassement de la tension nominale.

Les composants identifiés comme essentiels pour répondre à FSR\_1 incluent :

- Comparateur analogique (ACMP0) : Assure la détection du signal de surtension.
- LUTs (*Look-Up Tables*) : Implémentent la logique combinatoire pour générer le signal ASC.
- Broches GPIO : Permettent la communication des signaux d'entrée et de sortie nécessaires au déclenchement de la protection.

### 6.1 Les mode de défaillance

Lors de l'analyse FMEDA, nous avons identifié les modes de défaillance potentiels des composants impliqués dans la gestion de FSR\_1. Ces modes de défaillance ont été établis à l'aide du document **Renesas AN-CM-381** (*Determination of Failure In Time within the AEC-Q100 GreenPAK™ Family Automotive GreenPAK*) [1], qui fournit une liste exhaustive des modes de défaillance pour chaque type de composant du GreenPAK. Les modes de défaillance identifiés sont :

1. Défaillance des broches GPIO :
  - Une broche d'entrée, comme nOV, peut rester bloquée à un état logique haut ou bas, compromettant ainsi la détection correcte de la surtension.
  - Une broche flottante peut entraîner des erreurs de communication ou une perte de signal.
  - Ces modes de défaillance incluent :
    - Résistance de pull-up flottante.
    - Résistance de pull-up court-circuitée à la masse ou à l'alimentation.
    - Résistance de pull-down incorrectement sélectionnée à la place d'une résistance de pull-up.
2. Défaillance du comparateur ACMP0 :
  - Une défaillance de déclenchement ou une instabilité de la sortie peut empêcher l'activation de la protection ASC dans les délais impartis.
  - Les modes de défaillance spécifiques comprennent :
    - Non-déclenchement lorsque requis.
    - Fausse détection de déclenchement.
    - Sortie bloquée à un état haut ou bas.
    - Sortie flottante ou oscillante, provoquant une instabilité.
3. Défaillance des LUTs (Look-Up Tables) :
  - Une LUT bloquée (par exemple, bloquée à 1 ou 0) peut altérer la logique nécessaire à la génération du signal ASC.

Pour chaque mode de défaillance identifié, des solutions ont été mises en place afin de minimiser les risques comme :

- La surveillance continue des signaux par le microcontrôleur : Le microcontrôleur surveille en permanence les signaux critiques.
- La redondance logicielle : Des mécanismes comme le SM-01 permettent au microcontrôleur d'intervenir directement sur le signal ASC en cas de défaillance matérielle.

Cette approche garantit une couverture diagnostique élevée et une capacité à réagir efficacement, même en cas de défaillances critiques.

## 6.2 Calcul des FIT pour FSR\_1 en se basant sur l'exemple du document Renesas

Dans l'analyse de FSR\_1, nous avons déterminé les valeurs de FIT (*Failure In Time*) pour chaque composant critique en suivant une méthodologie similaire à celle décrite dans le document Renesas. Voici comment les valeurs ont été calculées :

### 1. Identification des modes de défaillance :

Pour chaque composant, les modes de défaillance possibles ont été répertoriés :

- Résistance pull-up/down flottante, court-circuitée à la masse ou à l'alimentation.
- Composants bloqués à 1 ou 0.
- Instabilité des sorties.

### 2. Répartition des défaillances :

Chaque mode de défaillance a été associé à un pourcentage de distribution. Par exemple, pour les broches GPIO chaque type de défaillance (flottante, court-circuitée, etc.) représente 20% du taux global de défaillance de cette broche.

### 3. Utilisation des données du fabricant :

Les données fournies par Renesas incluent des taux de défaillance globaux pour des éléments spécifiques, tels que :

- 0,6 FIT pour les broches GPIO.
- 0,74 FIT pour le comparateur ACMP0.
- 0,014 FIT pour les LUTs.

### 4. Calcul des FIT spécifiques :

Pour chaque mode de défaillance, le taux global de FIT est multiplié par le pourcentage de répartition du mode de défaillance. Par exemple :

Pour une broche GPIO avec 0,6 FIT et 20% de défaillances dues à une résistance pull-up flottante :

$$FIT\ spécifique = 0,6 \times 20\% = 0,12\ FIT$$

Pour une LUT bloquée avec 0,014 FIT et 50% de chances d'être bloquée à 1 ou à 0 :

$$FIT\ spécifique = 0,014 \times 50\% = 0,007\ FIT$$

### 5. Agrégation des valeurs de FIT :

Les FIT spécifiques pour chaque mode de défaillance sont additionnés pour obtenir le taux total de défaillance de chaque composant. Ensuite, les valeurs de FIT de tous les composants sont additionnées pour obtenir le FIT global du système.

### 6.3 Exemple détaillé pour nOV (broche GPIO) :

Taux global de FIT : 0,6 FIT.

- Résistance pull-up flottante : 20%
- Résistance pull-up court-circuitée à la masse : 20%
- Résistance pull-up court-circuitée à l'alimentation : 20%
- Résistance pull-down au lieu de pull-up : 20%
- Mauvais choix de résistance : 20%

Calcul pour chaque mode de défaillance :

- FIT spécifique =  $0,6 \times 20\% = 0,12$  FIT
- FIT total pour GPIO :  $0,12 + 0,12 + 0,12 + 0,12 + 0,12 = 0,6$  FIT

Résultats globaux pour FSR\_1 :

- Taux de défaillance global ( $\Sigma\lambda$ ) : 2,044 FIT.
  - GPIO: 1,2 FIT.
  - Comparateur : 0,74 FIT.
  - LUTs et DFF : 0,104 FIT.

Ces calculs montrent que chaque composant respecte les limites fixées par les standards, avec des taux de défaillance faibles.

### 6.4 Mécanismes de sécurité implémentés

Le principal mécanisme de sécurité pour FSR\_1 est SM-01 : Le microcontrôleur surveille le signal ASC en temps réel. En cas de défaillance, il peut générer un signal alternatif pour corriger ou compenser l'erreur, avec un taux de couverture de 99%

Les résultats de l'analyse FMEDA pour FSR\_1 montrent une conformité totale aux exigences ASIL C(D) :

- SPM (Taux de défaillance des points uniques) : 99,699%, démontrant une gestion efficace des défaillances individuelles.
- LFM (Taux de défaillance latente) : 100%, garantissant l'absence de défaillances non détectées.
- PMHF (Probabilité de défaillance par heure) : 0,006 FIT, confirmant une fiabilité élevée.

### 6.5 Conclusion

L'analyse approfondie de FSR\_1 a permis de valider la robustesse du circuit face aux exigences de sécurité. Les mécanismes de sécurité, tels que SM-01, assurent une détection rapide et une réponse efficace aux surtensions, même en cas de défaillances potentielles. Ces résultats renforcent la confiance dans la capacité du système à protéger les composants critiques de l'onduleur.

## 7. Analyses des FSR\_2 et FSR\_4

Les analyses des FSR\_2 et FSR\_4 ont suivi la même méthodologie que celle appliquée pour FSR\_1.

Les deux FSR ont montré une conformité complète aux exigences ASIL C(D) pour FSR\_2 et ASIL A(D) pour FSR\_4, grâce à des mécanismes de sécurité tels que SM-02 et SM-05, qui garantissent des couvertures diagnostiques élevées. Les résultats principaux incluent :

- SPFM et LFM : Des taux de couverture dépassant 99%, assurant une gestion robuste des défaillances individuelles et latentes.
- PMHF : Une probabilité de défaillance extrêmement faible, avec des valeurs inférieures à 0,01 FIT, confirmant la fiabilité du système.

Ces résultats montrent que les FSR\_2 et FSR\_4 respectent pleinement les exigences de sécurité imposées par la norme ISO 26262.

## 8. Analyse de FSR\_3 : Détection et déclenchement multiples

L'objectif de FSR\_3 est d'assurer une activation correcte des sorties de déclenchement LS-ASC ou HS-ASC dans un délai maximum de 100  $\mu$ s après la réception de plusieurs signaux d'erreur.

Pour analyser cette exigence, nous avons identifié les composants critiques impliqués dans le traitement des signaux multiples, tels que les LUTs (Look-Up Tables), les broches GPIO, et les blocs ASC. Comme pour les autres FSR, les modes de défaillance potentiels de ces composants ont été étudiés, et des mécanismes de sécurité (SM) ont été mis en place pour réduire les risques.

### Résultats de l'analyse

Les résultats montrent que le système présente une bonne couverture pour les défaillances latentes (LFM : 94,129%) et une faible probabilité de défaillance globale (PMHF : 2,652 FIT). Cependant, le SPFM (69,198%) est en deçà des attentes pour un niveau ASIL C(D), indiquant une insuffisance dans la gestion des défaillances individuelles critiques.

### Problématique identifiée dans FSR\_3

Malgré les mécanismes de sécurité en place, FSR\_3 ne respecte pas entièrement les exigences ASIL C(D). L'analyse a révélé deux problèmes majeurs :

Manque de supervision des signaux critiques :

- Les signaux DRV\_ASC\_ISO\_LS et DRV\_ASC\_ISO\_HS ne disposent pas de mécanismes de sécurité suffisants pour détecter les défaillances, tels qu'un état bloqué à 1 ou 0.
- L'absence de supervision appropriée de ces signaux empêche le système de réagir correctement à certaines conditions de défaillance.

Limitation des mécanismes de diagnostic : Les mécanismes actuels ne permettent pas une couverture diagnostique complète pour toutes les défaillances possibles. Cela expose le système à des risques non détectés.

### Solution proposée pour FSR\_3

Pour pallier ces insuffisances, nous proposons d'intégrer le microcontrôleur pour une surveillance et une correction active des signaux critiques :

Surveillance des signaux :

- Le microcontrôleur surveille en temps réel l'état des signaux de contrôle PS\_ASC\_SEL ainsi que des signaux DRV\_ASC\_ISO\_LS et DRV\_ASC\_ISO\_HS.
- En cas de détection d'une anomalie (blocage ou état flottant), le microcontrôleur peut réagir immédiatement pour corriger l'état des signaux concernés.

Activation de signaux alternatifs :

- Si une anomalie est détectée, le microcontrôleur active des signaux alternatifs pour remplacer ou compenser les signaux défectueux.
- Par exemple, si DRV\_ASC\_ISO\_LS ou DRV\_ASC\_ISO\_HS présentent une anomalie, le microcontrôleur peut activer des signaux correctifs pour maintenir la fonctionnalité du système.

## 9. Conclusion de la FMEDA

La FMEDA a permis d'évaluer la robustesse et la sécurité fonctionnelle de notre circuit de protection d'onduleur, en identifiant les modes de défaillance des composants critiques et en mettant en place des mécanismes de sécurité conformes à la norme ISO 26262. Les analyses FSR\_1, FSR\_2, et FSR\_4 ont montré que notre solution répond aux exigences ASIL C(D) et ASIL A(D) en termes de couverture diagnostique, fiabilité et réactivité. Cependant, l'analyse FSR\_3 a révélé des limitations dans la gestion des signaux critiques, pour lesquelles nous avons proposé une solution basée sur l'intervention du microcontrôleur, renforçant ainsi la sécurité et la fiabilité du système. En conclusion, la FMEDA a validé la sécurité fonctionnelle de notre circuit et nous a permis d'identifier des améliorations pour garantir une protection fiable des onduleurs.

## 10. WEBOGRAPHIE

[1] *Determination of Failure In Time within the AEC-Q100 GreenPAK™ Family Automotive GreenPAK*  
Disponible sur: <https://www.renesas.com/en/document/apn/cm-381-determination-failure-time-within-aec-q100-greenpak-family-automotive-greenpak?r=1563506>