



# NORME ISO 26262 AVEC UNE SOLUTION ALM

*Analyse des risques et ingénierie des exigences  
appliquées à la norme ISO 26262 avec Polarion ALM*

**Résumé :** La complexité des systèmes et équipements électroniques et électriques dans L'industrie automobile se poursuit à un rythme rapide et constant, et engendre de nouveaux défis en matière de sécurité. Pour y faire face et appréhender ses objectifs et contraintes dans ce domaine, l'industrie automobile a évolué en termes de normes et de processus au cours de ces dernières années. La norme ISO 26262, publiée en novembre 2011, définit les spécifications liées à la sécurité fonctionnelle des systèmes électriques et électroniques (E&E) des véhicules routiers. Elle recommande explicitement l'utilisation d'outils logiciels permettant de gérer les exigences relatives à la sécurité fonctionnelle et d'assurer leur traçabilité tout au long d'un cycle de vie. La norme ISO 26262 requiert également la qualification de tout élément logiciel ou matériel utilisé dans le cadre du développement d'un système.

Afin de répondre aux attentes des clients, la solution logicielle Polarion ALM permet de couvrir de manière complète les étapes de la partie 3 de la norme ISO 26262, consacrée à l'analyse et à la gestion des risques. Cette solution permet à toute organisation de faire de la gestion de la sécurité fonctionnelle une partie intégrante du cycle de vie des applications.

Après avoir exposé le concept de sécurité fonctionnelle, nous présenterons dans quelle mesure une solution logicielle ALM <sup>[1]</sup> peut aider les acteurs du secteur automobile à implémenter un processus conforme à la norme, et délivrer des produits de grande qualité assurant le niveau de sécurité attendu.

**Mots clé :** ISO 26262, Automobile, ASIL, Risque, Sécurité fonctionnelle

## 1. INTRODUCTION

Voici un exemple de la complexité croissante que connaît l'industrie automobile : selon certaines estimations, la conception d'une voiture haut de gamme nécessite presque 100 millions de lignes de code. Les logiciels embarqués commandent entre 70 et 100 unités de contrôle électronique (ECU) à base de microprocesseurs, destinées à la gestion d'équipements tels que le freinage ABS, les airbags, les lève-vitres électriques, la navigation GPS, les équipements de loisir, l'assistance de conduite électronique, l'aide au stationnement, etc.

Alfred Katzenbach, directeur informatique de Daimler rapporte que « Le système de radio et de navigation de la Mercedes-Benz Classe S requiert à lui seul plus de 20 millions de lignes de code, et cette voiture contient presque autant d'unités de contrôle électronique que le nouvel Airbus A320 (exception faite du système de divertissement en vol) ». La part logicielle dans l'automobile va continuer de croître en quantité et en complexité. Le cabinet conseil en stratégie Frost & Sullivan estime que, dans un proche avenir, la conception d'une automobile nécessitera entre 200 et 300 millions de lignes de code <sup>[2]</sup>.

Pour gérer cette complexité croissante, la norme ISO 26262 a été déduite de la norme de sécurité IEC 61508 pour répondre aux exigences spécifiques de sécurité appliquées à l'industrie automobile. Elle couvre les aspects de sécurité fonctionnelle appliqués à l'ensemble du processus de développement (spécification des exigences, conception, implémentation, intégration, vérification, validation et configuration). Associée à des modèles de processus tels que CMMI <sup>[3]</sup> ou SPICE <sup>[4]</sup>, elle permet d'atteindre efficacement les objectifs en matière de couverture de la sécurité fonctionnelle.

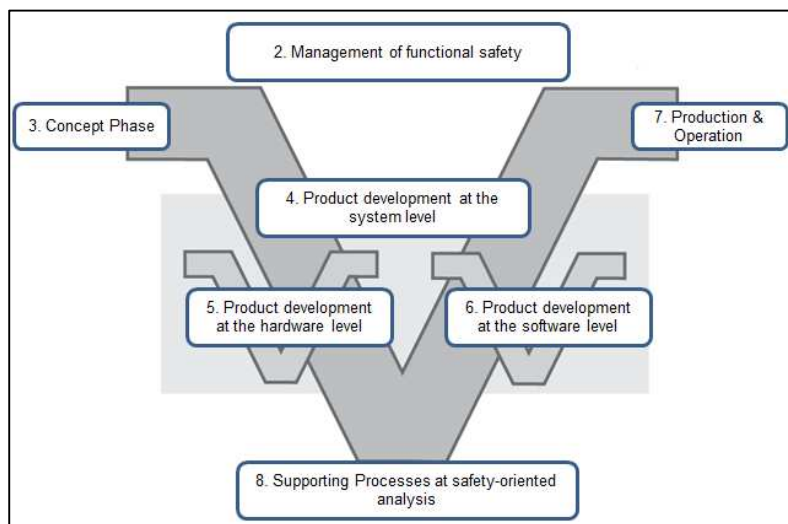
En résumé, les principaux défis de l'industrie automobile dans le secteur du développement des systèmes électriques et électroniques sont les suivants :

- ✓ Accroissement des fonctionnalités et de la complexité des équipements électroniques et électriques
- ✓ Une grande partie des nouvelles fonctions sont liées à la sécurité fonctionnelle de ces équipements
- ✓ Besoins croissants en gestion des risques afin d'obtenir un risque résiduel de niveau acceptable
- ✓ Mise en conformité avec la norme ISO 26262
- ✓ Implémentation de méthodes et de mesures adaptées au développement logiciel et supportées par des outils qualifiés

## 2. RELEVER LES DÉFIS

Les sociétés de l'industrie automobile investissent beaucoup de temps et d'argent dans le développement et l'amélioration de leurs processus et de leurs modèles. Elles sont donc, pour ce faire, à la recherche d'outils pour les aider dans leurs initiatives. Des solutions logicielles en matière de gestion des exigences et de gestion du cycle de vie des applications, telles que celles proposées par Polarion, sont parfaitement adaptées aux challenges actuels et à venir du développement automobile.

Ces solutions reposent sur un environnement logiciel de gestion du cycle de vie des applications, ou environnement ALM, hautement configurable et personnalisable. Elles fournissent par défaut des fonctionnalités de gestion des exigences et des risques qui garantissent une traçabilité complète et détaillée entre tous les artefacts clés du processus, avec une visibilité en temps réel sur l'avancement et l'état d'un projet.



La norme ISO 26262 s'appuie sur le modèle du cycle en V standard utilisé pour les différentes phases de développement d'un produit. Ainsi, Polarion a été adapté afin de prendre en charge la partie supérieure du cycle en V de la norme ISO 26262, à savoir les activités liées à l'analyse et à la gestion de la sécurité fonctionnelle.

Figure 1 : Modèle du cycle en V de la norme ISO 26262

## 3. CONCEPTS D'IMPLÉMENTATION POLARION ISO 26262

Un modèle de projet spécialisé permet de documenter le processus et de guider les utilisateurs au cours des différentes phases définie par l'ISO 26262. Il embarque sous forme de pages Wiki la connaissance du processus d'analyse et de gestion des risques (partie 3 de la norme ISO 26262) et livre les fonctionnalités pour gérer la sécurité fonctionnelle de bout en bout.

Le modèle projet intègre nativement :

- Des artefacts prédéfinis. Un artefact est tout élément de travail géré par les acteurs impliqués dans le processus, par exemple les événements (notion de hasard), les risques, les objectifs de sécurité, les exigences de sécurité fonctionnelle, les scénarios de tests, etc. Sous Polarion, le terme de « Work Item » est utilisé pour qualifier un artefact.
- Un workflow formalisant le processus d'analyse, d'évaluation des risques et de gestion des exigences
- Des champs personnalisés pour chaque type d'artefact (par exemple, exposition, gravité, contrôlabilité)

À partir des exigences de sécurité fonctionnelle spécifiées lors de la conception, des exigences techniques, matérielles et logicielles peuvent être déduites (parties 4, 5 et 6 de la norme ISO 26262). Ces artefacts peuvent également être gérés en intégralité au sein de la solution ALM. L'ensemble du processus est couvert via une plate-forme collaborative Web qui met en relation toutes les parties prenantes sur le cycle de vie du produit.

## Polarion ISO 26262 Template How-To

- Step 1: Hazard Identification
- Step 2: Hazard Classification
  - Step 2.1: Define Severity
  - Step 2.2: Define Exposure
  - Step 2.3: Define Controllability
- Step 3: ASIL Determination
- Step 4: Safety Goal Determination
- Step 5: Functional Safety Concept - Specification of Functional Safety Requirements
- Step 6: Specification of Safety Requirements (Technical, Software, Hardware Safety Requirements)

## Process

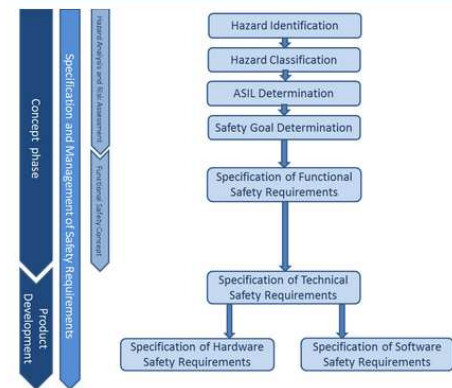


Figure 2 : Modèle de projet en V "How to" Polarion ISO 26262

Les outils qualifiés sous la norme ISO26262 doivent avoir acquis un niveau de confiance et disposer, par exemple, d'un guide d'utilisation et d'un document dans lequel ses fonctions sont décrites. Les pages Wiki sont très utiles pour mettre à disposition des utilisateurs un guide en ligne conçu pour répondre aux exigences de la norme. Par exemple, les pages Wiki Polarion expliquent les concepts d'analyse et de gestion des risques tels que définis dans la partie 3 de la norme ISO 26262, ainsi que l'utilisation du modèle ISO 26262.

Un exemple très représentatif d'une page Wiki est la page intitulée « *How-to Guide* », dans laquelle chaque étape du processus est expliquée clairement (par exemple, quels sont les éléments à prendre en compte pour identifier et décrire un « risque »). Un autre avantage de cette page est de fournir une définition et la liste de valeurs possibles de chaque attribut représentatif de l'ISO 26262 (par exemple, exposition, gravité, contrôlabilité). Ces paramètres sont essentiels, car ils permettent de déterminer le niveau de sécurité intégrée (ASIL) de chaque risque évalué.

### Step 2.2: Define Exposure

Exposure defines the Probability of a malfunction in connection with the operating state in relevant situations. In the following table the different classes of Exposure with the description, Probability of occurrence and an example are shown.

Class	Description	Probability of Occurrence	Example
<input type="checkbox"/> E0	incredible		
<input type="checkbox"/> E1	very low probability	not specified	Stand over railway crossing
<input type="checkbox"/> E2	low probability	less than 1% of average operating time	Driving with a trailer
<input type="checkbox"/> E3	medium probability	1 - 10% of average operating time	Refuel, Driving on a wet roadway
<input type="checkbox"/> E4	high probability	more than 10% of average operating time	Steer, Brake, Accelerate

Figure 3 : ISO 26262 : définition des facteurs clés

### Définition de l'item automobile

La définition de l'item a pour objectif de définir et de décrire l'élément automobile et son interaction avec son environnement et les autres items, selon la norme ISO 26262-3:2011 Clause 5. Le recueil et l'analyse de l'item automobile et de tout autre artefact associé (risque, objectif de sécurité, exigence de sécurité, etc.) s'effectue dans des documents Web, partagés entre tous, où certains contenus peuvent être marqués comme Work Item.

**2.5 Interfaces and Boundaries**

**2.6 Functional Requirements**

Add references to functional requirements or functional requirements documents

- EPB-198 - apply and disengage the parking brake by a touch button - no additional handbrake
- EPB-199 - "hold" the car securely on any incline
- EPB-200 - hill start assistance (automatic release)

**Work Item Properties**

EPB-198 - apply and disengage the parking brake by a touch button - no additional handbrake...

Properties

Severity:  Should Have

Status:  Draft

Links

has parent

- EPB-187 - Major Features

Documents

This Work Item is contained in

Business Specification and referenced in:

- Item Definition (this document)

Figure 4 : Définition d'élément selon la norme ISO 26262-3:2011 Clause 5 dans les documents LiveDoc Polarion

Cette méthode de capture d'une définition d'item directement à partir de documents formels offre le meilleur de deux mondes : utilisabilité des documents et processus de gestion piloté par les données.

Les analystes métier et les ingénieurs en gestion des exigences travaillant déjà à partir de documents n'ont besoin, ni de changer leurs habitudes, ni de renoncer à des fonctionnalités importantes et trouvent dans l'outil ALM une facilité d'utilisation équivalente, voire supérieure. Tout utilisateur peut exploiter les fonctions mises à sa disposition pour gérer les données du référentiel en suivant le processus prédéfini (workflow).

Les managers et les personnes responsables des questions de conformité disposent des rapports dont ils ont besoin. L'ensemble de l'organisation bénéficie d'une réelle amélioration en matière d'efficacité, de transparence et de communication.

À tout moment au cours du processus de définition de l'item au sein du document, un contenu peut être marqué en tant que Work Item, qui est alors créé dans le référentiel sous-jacent. Ceci permet à l'ensemble de l'équipe de bénéficier de toutes les fonctionnalités du Workflow et de gestion de projet fournies par la solution ALM. Les rédacteurs ou relecteurs des documents peuvent continuer à travailler le contenu.

Un seul document peut contenir différents types de Work Items. Par exemple, il peut en effet être intéressant de faire référence à la fois aux exigences de sécurité fonctionnelle et aux scénarios de test qui leurs sont associés.

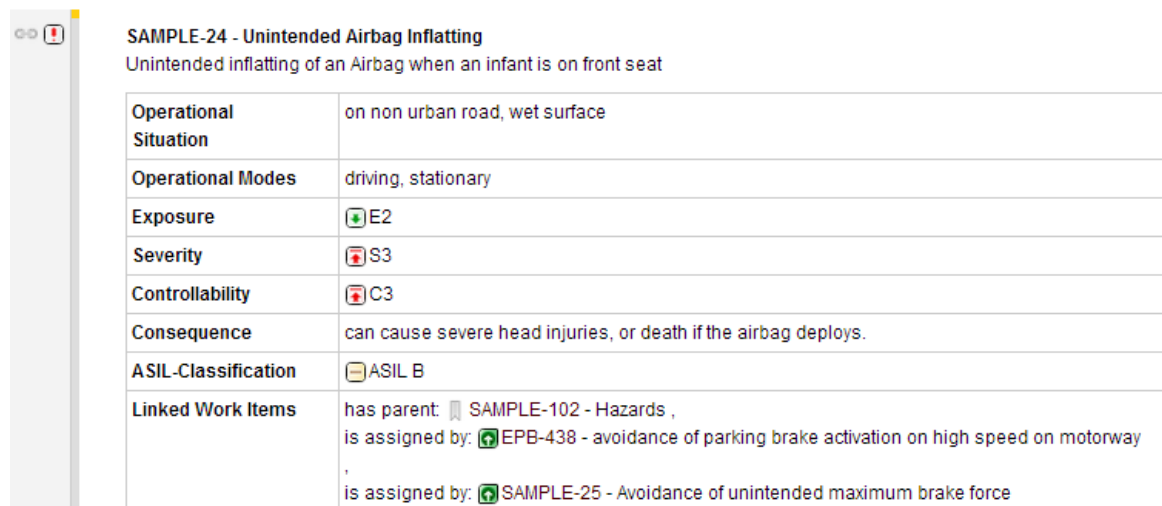
Un historique permet de mieux comprendre les modifications apportées d'une version à une autre pour chaque document de spécifications. Pour collaborer sur son contenu, un utilisateur doit pouvoir exporter et partager le document avec des intervenants externes n'ayant pas accès au référentiel, puis le réimporter dans le système. Les modifications sont alors réintégréées au document, avec mise à jour automatique de l'historique.

#### 4. PROCESSUS D'ANALYSE ET D'ÉVALUATIONS DES RISQUES

Dans la norme ISO 26262, le processus d'analyse et d'évaluation des risques se décompose en quatre étapes :

##### *Étape 1 : Identification du risque*

L'objectif consiste à identifier et à décrire les situations et les modes opératoires dans lesquels le dysfonctionnement d'un élément peut se produire. Par exemple, le déverrouillage accidentel du frein à main d'une voiture en stationnement peut constituer un risque potentiel.



SAMPLE-24 - Unintended Airbag Inflatting	
Unintended inflatting of an Airbag when an infant is on front seat	
Operational Situation	on non urban road, wet surface
Operational Modes	driving, stationary
Exposure	E2
Severity	S3
Controllability	C3
Consequence	can cause severe head injuries, or death if the airbag deploys.
ASIL-Classification	ASIL B
Linked Work Items	has parent: SAMPLE-102 - Hazards , is assigned by: EPB-438 - avoidance of parking brake activation on high speed on motorway , is assigned by: SAMPLE-25 - Avoidance of unintended maximum brake force

Figure 5 : Définition d'un Work Item de type risque avec attributs et liens

Il faut ici lister les situations de conduite et de fonctionnement, détailler les modes de défaillance entraînant des risques dans des situations spécifiques, se concentrer ici uniquement sur les événements possibles attachés à l'item, sans chercher encore à réduire le risque. Pour ce faire, il est nécessaire d'impliquer des personnes possédant de bonnes connaissances et une expérience du domaine. Une plate-forme Web unifiée permet une véritable collaboration entre les différents intervenants.

Des techniques appropriées (basées par exemple sur le "brainstorming", sur l'analyse des modes de défaillance, de leurs effets et de leur criticité - méthode AMDEC - ou sur des listes de contrôle) peuvent être implémentées et

suivies dans l'outil ALM, de manière à identifier systématiquement les risques.

### Étape 2 : Classification du risque

Tout risque identifié doit être classifié via trois indicateurs afin de déterminer les classes de risque : la probabilité d'exposition en situation de conduite et de fonctionnement, l'estimation de la contrôlabilité et l'estimation de la gravité potentielle.

La probabilité d'exposition définit la possibilité d'un dysfonctionnement en lien avec l'état opérationnel dans les situations considérées. Les classes d'exposition, ainsi que leur description et probabilité d'occurrence, sont documentées dans le « *How-to Guide* ». La probabilité d'exposition se mesure de E0 à E4 (inimaginable - hautement probable). Par exemple, à quelle fréquence un airbag explose-t-il alors qu'un enfant est assis sur le siège avant ?

La gravité représente la mesure de l'étendue des dommages causés à une personne dans une situation spécifique. Elle se mesure de S0 à S3 (aucune blessure - blessures potentiellement mortelles). Par exemple, quelle sera la gravité de la blessure de l'enfant ?



Figure 6 : Classification de la gravité d'un Work Item de type risque

La contrôlabilité définit la prévention des dommages par une réaction rapide du conducteur (ou des occupants du véhicule). Elle se mesure de C0 à C3 (généralement contrôlable - difficile à contrôler ou à gérer). Par exemple, l'enfant ou le conducteur peut-il contrôler l'explosion de l'airbag ?

### Étape 3 : Détermination de l'ASIL



Un ASIL (Automotive Safety Integrity Level) est déterminé pour chaque risque en fonction des valeurs des paramètres gravité, probabilité d'exposition et contrôlabilité.

Figure 7 : ISO 26262 : Détermination de l'ASIL

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Comme le montre ce tableau, chaque risque est classé, selon un niveau d'exigence en termes de sécurité, de A à D (D représentant le risque le plus élevé) ou QM (Quality Management, soit sans influence sur la sécurité).

Figure 8 : ISO 26262 : Classes ASIL

Chaque Work Item ISO 26262 du modèle projet Polarion dispose de sa propre définition de cycle de vie ou workflow. Un workflow est un ensemble d'états, de transitions entre états, de conditions de transition et de dépendances par lesquels passe un Work Item au cours de son cycle de vie. Le modèle projet Polarion ISO 26262 formalise ainsi le processus qui doit être suivi par les analystes pour obtenir une détermination automatique du niveau ASIL.

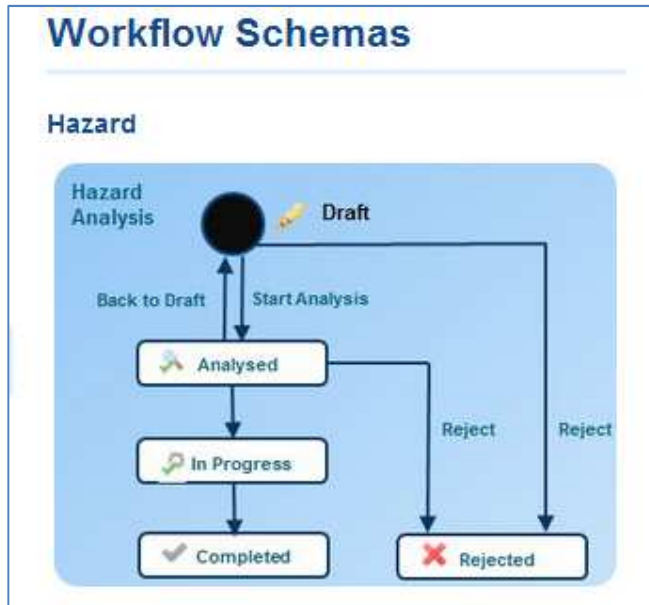


Figure 9: Workflow personnalisé pour un Work Item de type risque

#### Étape 4 : Détermination des objectifs de sécurité

Un ou plusieurs objectifs de sécurité doivent être déterminés pour chaque risque. Un objectif de sécurité est une exigence de haut niveau résultant du processus d'analyse de risque. Par exemple, le fait que l'airbag se déclenche uniquement en cas de collision peut constituer un objectif de sécurité. Le comportement requis ainsi défini permet de diminuer les risques et d'accroître la sécurité.

Si plusieurs risques correspondent à l'objectif de sécurité, l'ASIL le plus élevé doit être affecté. Sous Polarion, l'objectif de sécurité est représenté en tant que Work Item, et comporte tous les attributs personnalisés nécessaires à sa définition complète, un workflow qui lui est propre, et des liens prédéfinis vers les autres types d'artefacts.

Le mécanisme de lien facilite la gestion du flux complet d'exigences, depuis la phase de développement du concept jusqu'aux exigences logicielles/matérielles et activités connexes, produits, éléments de risque et/ou scénarios de test. Un lien se distingue par son nom (*est lié à, implémente, vérifie, etc.*) et peut avoir plusieurs sémantiques.

L'ASIL du nouvel objectif de sécurité est défini en fonction de la détermination ASIL du risque correspondant. Les utilisateurs peuvent modifier la valeur de l'ASIL attachée à l'objectif de sécurité, dans le respect des règles du Workflow défini : la modification de l'ASIL ne sera plus possible après finalisation et approbation de la révision de l'artefact.

ID	Title	Status	Assignee(s)	Time Point	Created	Remaining E
EPB-320	avoidance of unintended parking brake release	Reviewed			2013-04-11 11:11	1E
EPB-32	Automatic Brake Lock in parking position				2013-04-11 11:11	1E
EPB-	Test: Automatic Brake Lock in parking position				2013-04-11 11:11	1E
EPB-	Implement: Automatic Brake Lock in parking position			Iteration 1 (20'	2013-04-11 11:11	5d

**EPB-319** +  
 ↑ e-9 **EPB-320 - avoidance of unintended parking brake release**  
 ↑ EPB-321 +

Type: Safety Goal  
 Author: Administrateur Système  
 Project: Electronic Parking Brake

Assignee(s): Administrateur Système  
 Status: Reviewed  
 Resolution:

ASIL-Classification: ASIL C

Figure 10 : Arborescence hiérarchique avec objectif de sécurité/ exigence de sécurité/scénario de test/ tâche

Lier les Work Items est la clé pour tirer profit des fonctions de traçabilité et d'analyse d'impact présents dans l'outil ALM. Mesurer l'impact de la modification d'un risque, d'une exigence, sur différents produits et/ou variantes de produits, ou encore identifier les exigences de sécurité orphelines (sans exigence fonctionnelle associée), ne doit pas être limité par la portée du projet ; il convient donc d'avoir la capacité à lier des Work Item non seulement au sein d'un même projet, mais également entre différents projets ou même différents référentiels.

## 5. CONCEPT DE SÉCURITÉ FONCTIONNELLE

### *Spécification des exigences de sécurité fonctionnelle*

La première étape du concept de sécurité fonctionnelle consiste à décliner les exigences à partir des objectifs de sécurité.

À l'image du Work Item Objectif de Sécurité, le type de l'élément de travail « Exigence de sécurité fonctionnelle » comporte tous les attributs personnalisés nécessaires à sa définition complète, un workflow qui lui est propre, et des liens prédéfinis vers les autres types de Work Item.

L'ASIL de la nouvelle exigence de sécurité fonctionnelle est défini en fonction de l'ASIL de ou des objectifs de sécurité correspondants. Dans les cas où plusieurs objectifs sont liés à l'exigence, l'ASIL le plus élevé doit être affecté. Les utilisateurs ont la latitude pour modifier l'ASIL déterminé automatiquement sur cette base de calcul, à nouveau tant que le processus d'approbation de l'exigence n'est pas finalisé.

### *Spécification des exigences techniques, matérielles et logicielles de sécurité*

Au cours du développement du produit, les exigences de sécurité fonctionnelle sont affinées en fonction d'exigences techniques, matérielles et/ou logicielles. Ainsi, on peut concevoir qu'un système de capteurs détecte la présence d'un enfant sur le siège avant et désactive l'airbag.

L'ASIL de l'exigence de sécurité technique devra alors être affecté à l'exigence de sécurité fonctionnelle correspondante. Si plusieurs exigences de sécurité fonctionnelle correspondent à l'exigence de sécurité technique, l'ASIL le plus élevé doit être affecté.

La valeur de l'ASIL de la nouvelle exigence de sécurité technique est déterminée selon la valorisation de l'ASIL de l'exigence de sécurité fonctionnelle liée en amont. Il y a donc un héritage de l'ASIL, mais un changement reste possible dans le respect des règles de la norme.

## 6. AUDIT, TRAÇABILITÉ ET ANALYSE D'IMPACT

Les rapports de traçabilité permettent d'obtenir une transparence totale tout au long du cycle de vie d'un produit, de la gestion des exigences métiers à l'assurance qualité en passant par le développement. La traçabilité est mesurée en s'appuyant sur les liens définis entre les Work Items. Avec la norme ISO 26262, l'analyse et la révision bénéficient de différentes vues, de rapports et de pages Wiki qui permettent de vérifier la manière dont les risques, les objectifs de sécurité et les exigences de sécurité, fonctionnelles et techniques, ont été pris en compte.

### Traceability: Hazard - Safety Goal - Functional Safety Requirement

type:hazard AND projectId:ElectronicParkingBreak	type:safetygoal	type:safetyrequirement AND reqtype:functional
<ul style="list-style-type: none"> <li>EPB-319 - Unintended Parking Deactivation</li> </ul>	<ul style="list-style-type: none"> <li>EPB-434 - Parking Deactivation Control</li> <li>EPB-320 - avoidance of unintended parking brake release</li> </ul>	<ul style="list-style-type: none"> <li>EPB-321 - Automatic Brake Lock in parking position</li> </ul>
<ul style="list-style-type: none"> <li>EPB-439 - Unintended Parking Activation</li> </ul>	<ul style="list-style-type: none"> <li>EPB-435 - adress</li> </ul>	
<ul style="list-style-type: none"> <li>SAMPLE-24 - Unintended Airbag Inflating</li> </ul>	<ul style="list-style-type: none"> <li>SAMPLE-25 - Avoidance of unintended maximum brake force</li> <li>EPB-438 - avoidance of parking brake activation on high speed on motorway</li> </ul>	<ul style="list-style-type: none"> <li>SAMPLE-27 - Vehicle velocity signal must be read in</li> <li>SAMPLE-26 - Vehicle velocity must be plausible</li> </ul>

Figure 11 : Traçabilité entre artefacts (Work Items) de sécurité

Ce rapport de traçabilité, dynamique, fiable, et ergonomique permet également de déterminer l'impact potentiel des changements sur d'autres exigences. Il est d'une grande aide dans l'évaluation de la couverture et facilite la

validation des liens ; par exemple, l'analyste peut vérifier instantanément si à chaque objectif de sécurité correspond au moins une exigence de sécurité fonctionnelle, ou encore d'évaluer les règles ISO 26262 telles que l'héritage ASIL.

Safety Goal	Hazard
EPB-434 - Parking Deactivation Control ASIL-Classification: ASIL A	EPB-319 - Unintended Parking Deactivation ASIL-Classification: ASIL C
SAMPLE-25 - Avoidance of unintended maximum brake force ASIL-Classification: ASIL B	SAMPLE-24 - Unintended Airbag Inflating ASIL-Classification: ASIL B
EPB-438 - avoidance of parking brake activation on high speed on motorway ASIL-Classification: ASIL C	SAMPLE-24 - Unintended Airbag Inflating ASIL-Classification: ASIL B
EPB-435 - adress ASIL-Classification: ASIL C	EPB-439 - Unintended Parking Activation ASIL-Classification: ASIL C
EPB-320 - avoidance of unintended parking brake release ASIL-Classification: ASIL C	EPB-319 - Unintended Parking Deactivation ASIL-Classification: ASIL C

Figure 12 : Mesure de l'héritage ASIL entre les objectifs de sécurité et les risques

L'utilisation d'une plate-forme ALM collaborative facilite également l'audit de la sécurité fonctionnelle. Chaque modification d'artefact est tracée et enregistrée via le système de gestion de version intégré. Une piste d'audit complète (qui, quand, quoi, pourquoi) est disponible en permanence. Les parties prenantes peuvent être automatiquement notifiées des modifications apportées, par l'envoi d'emails avec un format structuré et/ou par la mise à jour d'une liste des activités sur leur page personnelle. Il est ensuite facile de savoir qui a modifié une analyse de risques, à quel moment ces changements ont été apportés et ce qui est/a été fait pour mitiger les risques.

## 7. CONCLUSION

Disposer d'une stratégie/méthodologie structurée et parfaitement définie est indispensable pour garantir une conformité avec la norme ISO 26262 ; un outil certifié ALM peut constituer une aide précieuse pour appliquer le processus. L'implémentation d'un modèle tel que celui de Polarion représente une base et un point de départ pour gérer la complexité et prendre en charge l'intégration de la sécurité fonctionnelle dans les applications de l'industrie automobile.

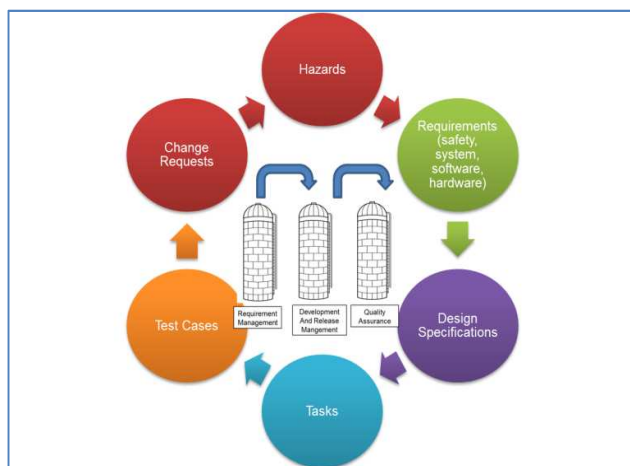


Figure 13 : Renforcement de la collaboration et réduction des silos

La conformité à la norme ISO 26262 est mise en évidence à travers une implémentation complète des phases d'analyse et d'évaluation des risques, de détermination des objets qualité et des exigences de sécurité associées, mais plus globalement à travers toutes les étapes du cycle de vie de développement d'un produit, d'un logiciel ou d'un système, depuis la définition du concept jusqu'au déclassement du produit.

La solution Polarion ALM, par sa couverture fonctionnelle et son approche centralisée « Web Centric », renforce la collaboration entre toutes les parties prenantes et contribue à l'élimination des silos entre les activités.

Bien entendu, la conformité totale avec la norme ISO 26262 nécessite d'aller plus loin que la phase d'analyse de la sécurité fonctionnelle. Les exigences fonctionnelles, matérielles et logicielles qui représentent un élément essentiel du processus d'évaluation de la sécurité, peuvent être gérées intégralement avec Polarion ALM depuis leur recueil jusqu'à leur vérification et validation (V&V), en passant par leur implémentation (codage). Comme tout autre artefact (Work Item), les défauts, les demandes de changements, les scénarios de test et les tâches orientées développement sont gérées et liées aux objectifs et aux exigences de sécurité.



Le suivi et la gestion du cycle de vie complet du produit ne peuvent pas être assurés par un outil unique ; généralement, un Framework <sup>[5]</sup> est mis en place et une solution telle que Polarion joue un rôle central et fédérateur au cœur de cet ensemble cohérent. Polarion conçu sur Eclipse s'appuie sur une architecture ouverte dotée d'une API Java, d'interfaces Web Services, XML <sup>[6]</sup>, SOAP <sup>[7]</sup> permettant de s'intégrer avec de nombreux logiciels tiers comme les IDEs <sup>[8]</sup>, les automates de tests, les environnements de modélisation (UML <sup>[9]</sup>, Simulation et conception basée sur des modèles), les systèmes de suivi des défauts, etc. Ces intégrations permettent de synchroniser et partager les données entre les environnements, et d'apporter une traçabilité complète et bidirectionnelle entre les éléments gérés par les différents logiciels.

Figure 14 : Certification TUV Nord



En novembre 2012, Polarion a été certifié IEC 61508 et ISO 26262 par le TÜV NORD (Allemagne) pour l'ensemble du cycle de vie des applications. Au travers de cette certification accordée par une autorité tierce, les processus de développement logiciel de Polarion Software sont en conformité avec le niveau ASIL le plus élevé (ASIL-D) tel que défini dans la norme ISO 26262. En outre, tout système logiciel et matériel développé à l'aide des processus Polarion est considéré comme répondant aux exigences de sécurité fonctionnelle de la norme ISO 26262.

Ainsi, la solution certifiée ISO 26262 de Polarion Software aide les sociétés du secteur automobile à réduire considérablement leurs efforts en matière d'évaluation de la conformité et de certification des outils employés.



#### À propos de l'auteur :

Responsable technique au sein de l'éditeur de logiciels Polarion Software, Serge Dubois possède plus de 15 années d'expérience dans les domaines de l'ingénierie des exigences, du développement d'applications, et a développé une expertise sur toutes les activités propres aux tests et à la validation des logiciels. Il a œuvré auparavant chez plusieurs éditeurs mondiaux de logiciels proposant des solutions pour couvrir les phases projet liées à la qualité logicielle. En tant que garant de la cohérence technique des solutions proposées par Polarion Software, il accompagne et conseille les clients de Polarion Software dans l'optimisation de la gestion du cycle de vie des applications, que ce soit autour d'une démarche outillée ou de l'amélioration de leur processus.

[1]ALM (Application Lifecycle Management) : processus global de gestion du cycle de vie d'un logiciel

[2]Robert N. Charette : IEEE Spectrum, février 2009

[3]CMMI (Capability Maturity Model Integration) : ensemble structuré de bonnes pratiques pour optimiser le développement logiciel

[4]SPICE (Software-Process Improvement and Capability Determination) : évaluation et amélioration des processus de développement

[5]Framework : Socle de logiciels, ou architecture formant un ensemble cohérent

[6] XML (Extensible Markup Language) : est un langage de balisage générique permettant de définir différents langages avec chacun leur vocabulaire et leur grammaire

[7] SOAP (Simple Object Access Protocol) est un protocole de RPC (Remote Procedure Call) orienté objet bâti sur XML.

[8]IDE (Integrated Development Environment) : environnement de développement intégré

[9]UML (Unified Modeling Language) : Langage de modélisation unifié de l'OMG