SÉCURISER

UNE NOUVELLE APPROCHE POUR LES FONCTIONS SIL

Le SIL est un indicateur essentiel pour la conception d'une fonction de sécurité et pour la détermination des périodes de test de maintenance préventive. Il ne fournit cependant pas une information suffisante pour l'exploitation des fonctions instrumentées de sécurité. SPC Consultants propose de compléter l'approche actuelle du SIL en introduisant un second indicateur intitulé SCL (Safety Criticality Level).

Claude Tourniaire, membre de l'équipe fondatrice de SPC Consultants et associé, société d'ingénierie et de prestations dédiées aux processus et aux systèmes de pilotage et d'information de la production, de la qualité et de l'innovation.

Pour les industries de process à risques, des approches dites « *SIL* » (Safety Integrity Level selon la norme IEC61511) sont utilisées depuis plus de 20 ans. Le niveau SIL d'une fonction instrumentée de sécurité (SIF Safety Instrumented Function) indique le niveau de confiance dans le bon fonctionnement de la fonction, c'est-à-dire sa disponibilité au moment de la sollicitation (cas des sollicitations rares ce qui correspond à la majorité des cas pour les industries de process).

Or si le SIL est un indicateur indispensable pour la conception d'une fonction de sécurité et pour la détermination des périodes de test de maintenance préventive, il ne donne pas une information suffisante pour l'exploitation des fonctions instrumentées de sécurité. En particulier le niveau de SIL ne donne pas d'aide quant à la criticité en exploitation de la fonction de sécurité en cas de défaillance d'un instrument ou de pose d'un bipasse de maintenance. De plus, il ne permet pas de prioriser les interventions de maintenance.

SPC Consultants propose de compléter l'approche actuelle du SIL en introduisant un second indicateur nommé SCL (Safety Criticality Level). Ces deux indicateurs SIL et SCL utilisés conjointement permettent de répondre à l'ensemble des interrogations liées à la conception, l'exploitation et la maintenance d'un système instrumenté de sécurité

ANALYSES DES RISQUES ET APPROCHE DE TYPE LOPA

La première étape d'une approche IEC61511 consiste en l'analyse des risques et l'allocation des niveaux de réduction de risque aux différentes barrières de chacun des scénarios de risque.

Pour les procédés à risques, l'approche recommandée est de type LOPA (Layer Of Protection Analysis). Cette approche probabiliste consiste en l'analyse de la réduction progressive d'un risque par la mise en place d'une succession de barrières efficaces et indépendantes et qui, ensemble, permettent de réduire le risque jusqu'à son acceptabilité.

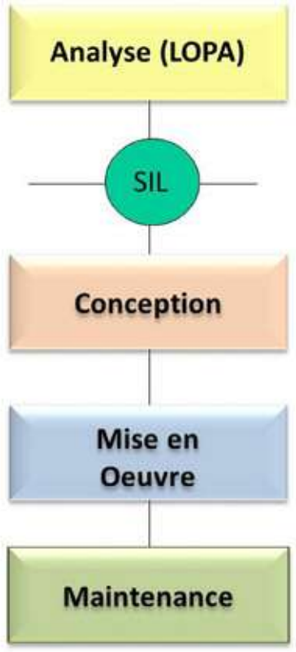

Figure 1 : cycle simplifié IEC 61511

Les barrières protectives permettent de réduire la gravité de l'événement redouté et les barrières préventives permettent d'en réduire la fréquence

Chaque barrière préventive efficace dans le scénario de risque réalise un saut de fréquence. Le FRR (Facteur de Réduction du Risque) donne la mesure de cette réduction à travers la formule :

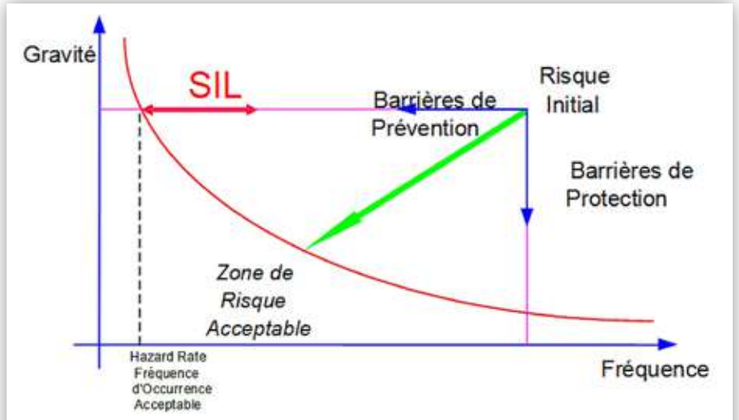

Figure 2 : principe d'une analyse LOPA

FRR = F_{ini} / F_{red} (Fréquence initiale / Fréquence réduite).

La norme IEC61511 utilise le PFDavg (Probability of Failure on Demand average) avec : PFDavg = 1 / FRR = Fred / Fini.

Le niveau SIL d'une fonction instrumentée de sécurité correspond à une classe de réduction du risque ou de PFDavg avec pour un SIL1 un FRR compris entre 10 et 100, pour un SIL2 un FRR entre 100 et 1000 et pour un SIL3 un FRR entre 1000 et 10000. (Le niveau SIL4 de la norme n'est pas repris ici car il doit être absolument évité en projet et relève de prescriptions spécifiques). Le niveau de SIL requis d'une SIF est ainsi donné par la longueur du segment associé à la barrière dans le diagramme gravité – fréquence.

Cette approche LOPA peut favorablement être intégrée à un outil de type Hazop (Hazard and Operability), ce qui permet un gain de temps et d'efficacité en projet sous la condition de réaliser une analyse des scénarios suffisamment précise pour que chacune des barrières utilisées dans un scénario de risque soit efficace pour ce scénario.

CONCEPTION DES BARRIÈRES INSTRUMENTÉES DE SÉCURITÉ

Le niveau de SIL requis (ou de FRR requis de façon équivalente) obtenu par l'approche LOPA permet ensuite à travers des calculs de fiabilité et la prise en compte des types d'instruments et des contraintes architecturales de définir :

- L'architecture capteur et actionneur (schéma de redondance)
- Les comportements sur défaut
- Les périodes de test selon l'efficacité retenue pour les tests et la stratégie des tests (manuels, automatiques…)

Une approche de type diagramme de fiabilité (ou diagramme de succès) est particulièrement adaptée pour cette étape par l'identification simple des points faibles d'une fonction et la facilité d'amélioration ainsi apportée.

INTRODUCTION DU COÛT ASSOCIÉ À UN RISQUE

Pour aller plus loin dans l'analyse des barrières, nous utilisons la notion de coût associé à un risque. Ce coût peut être obtenu à travers l'échelle de gravité utilisée pour le projet lorsque cette échelle intègre les impacts sur les pertes de production et l'endommagement des équipements. Ainsi on a : ***Coût Risque=Fonction(Gravité)***

A noter que le coût associé à un risque doit prendre en compte le fait que lorsqu'un événement relève d'une gravité élevée et donc de conséquences particulièrement graves, celui-ci sera convenablement majoré pour prendre en compte les impacts sur les personnes internes et externes au site, sur les équipements, sur l'environnement et sur l'image de l'entreprise.

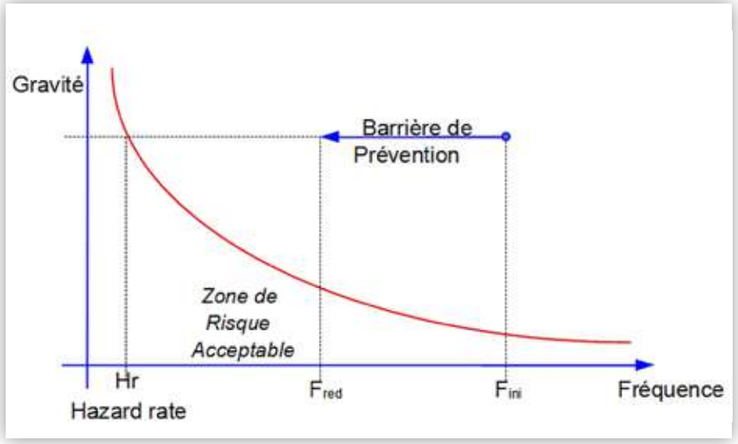

Figure 3 : la réduction du risque par une barrière préventive

Le « *Gain* » associé à une barrière par la réduction du Coût du risque s'exprime alors par :

Gain Annuel Barrière= Coût Risque*Fini*(1-1/FRR)

Bien entendu, nous utilisons ici le terme de « *Gain* » pour une information qui ne correspond qu'à une réduction du coût lié aux risques et en faisant l'hypothèse que chaque risque peut être quantifié par un coût.

LA CRITICITÉ D'UNE FONCTION DE RÉDUCTION DU RISQUE

Le niveau de criticité d'une fonction de réduction d'un risque est nommé SCL (Safety Criticality Level). Il donne l'impact de sécurité en cas de perte d'une fonction de sécurité (sur défaillance ou sur activation d'un bipasse de maintenance par

Conclusions et recommandations

L'utilisation conjointe du SIL et du SCL permet de couvrir l'ensemble des étapes du cycle de vie des sécurités instrumentées : conception, exploitation et maintenance. L'utilisation du SCL permet une meilleure prise en compte de l'importance opérationnelle d'une barrière et une priorisation justifiée des actions d'exploitation et de maintenance. Il est recommandé d'utiliser une méthode de type LOPA de quantification des risques (par exemple intégrée à une approche HAZOP), d'utiliser le SIL pour la conception initiale des fonctions instrumentées de sécurité et pour la détermination des périodes de test, et d'utiliser le SCL pour leur exploitation et leur maintenance (mesures compensatoires, priorisation des interventions…)

Fonction instrumentée de sécurité	SIL	SCL
Conception	- Architecture de la SIF - Comportement sur défaut	- Séparation EIPS / non EIPS - Analyse ALARP / ROI
Exploitation		- Renforcement des mesures compensatoires voire arrêt d'exploitation
Maintenance	- Périodes de test	- Priorisation des interventions de dépannage (réduction de la durée de pose des bipasses de maintenance) - Priorisation des tests périodiques si nécessaire

exemple). Le SCL est défini pour une barrière dans un scénario de risque sous l'hypothèse que les autres barrières du scénario soient opérationnelles : .

Le SCL varie typiquement entre 1 et 5 du plus faible au plus élevé. Lorsque la même barrière participe à plusieurs scénarios de risque, le SCL peut être défini par :

SCL= log10 (∑_ Scénarios Gain Annuel Barrière)

On peut considérer qu'une barrière disposant d'un SCL >3 et intervenant dans au moins un scénario de risque élevé (atteinte significative aux personnes) est une barrière *« Forte »*.
Ainsi, alors que le SIL ne reflète que le FRR, le SCL prend en compte à la fois le niveau de gravité de l'événement redouté et les autres barrières concourant à la réduction du risque pour les scénarios concernés.

LA SÉPARATION EIPS / NON EIPS DES BARRIÈRES

La réglementation a introduit la notion de MMRi (Mesure de Maîtrise des Risques instrumentée). Le texte UFIP / UIC DT93 donne les règles à suivre pour obtenir une présomption de conformité réglementaire.

Pour les barrières instrumentées autres que les MMRi et en particulier lorsqu'il s'agit de la protection des personnels du site, certains sites maintiennent une séparation entre barrières dites EIPS et celles qui ne sont pas EIPS, de façon à prioriser les actions d'exploitation (mesures compensatoires sur anomalie) et de maintenance (réparations et tests). L'utilisation du SCL conjointement avec le niveau de gravité permet de réaliser cette catégorisation en identifiant comme EIPS les barrières *« Fortes »*.

A noter que la notion de SCL n'est pas limitée aux fonctions instrumentées de sécurité et s'applique à toutes les barrières soumises à défaillances probabilistes (alarmes, procédures, interlocks, SIF, sécurités mécaniques…)

TEMPS DE RETOUR ET NOTION D'ALARP

Lors de l'analyse LOPA, on peut légitimement se poser la question du temps de retour (ROI Return On Investment) d'une barrière qui serait ajoutée ou comparer économiquement différentes voies possibles de réduction du risque.
Le SCL donne le log du gain annuel d'une barrière de sécurité . Si le coût global (CAPEX + OPEX) d'une barrière supplémentaire est inférieur au gain annuel sur la durée d'exploitation de l'installation (typiquement 20 à 30 ans), alors la décision d'investissement pourra être positive : .

*Coût Global Barrière<Gain Annuel Barrière*Durée d'exploitation de l'installation*

Cette analyse est complémentaire de celle conduisant à l'acceptabilité du risque qui doit être atteinte dans tous les cas.
La notion d'ALARP (As Low As Reasonably Practicable) telle que définie par les anglo-saxons correspond à cette approche : au-delà de l'acceptabilité, on décide de retenir une ou plusieurs barrières supplémentaires si le critère de coût défini ci-dessus est rempli. ▬

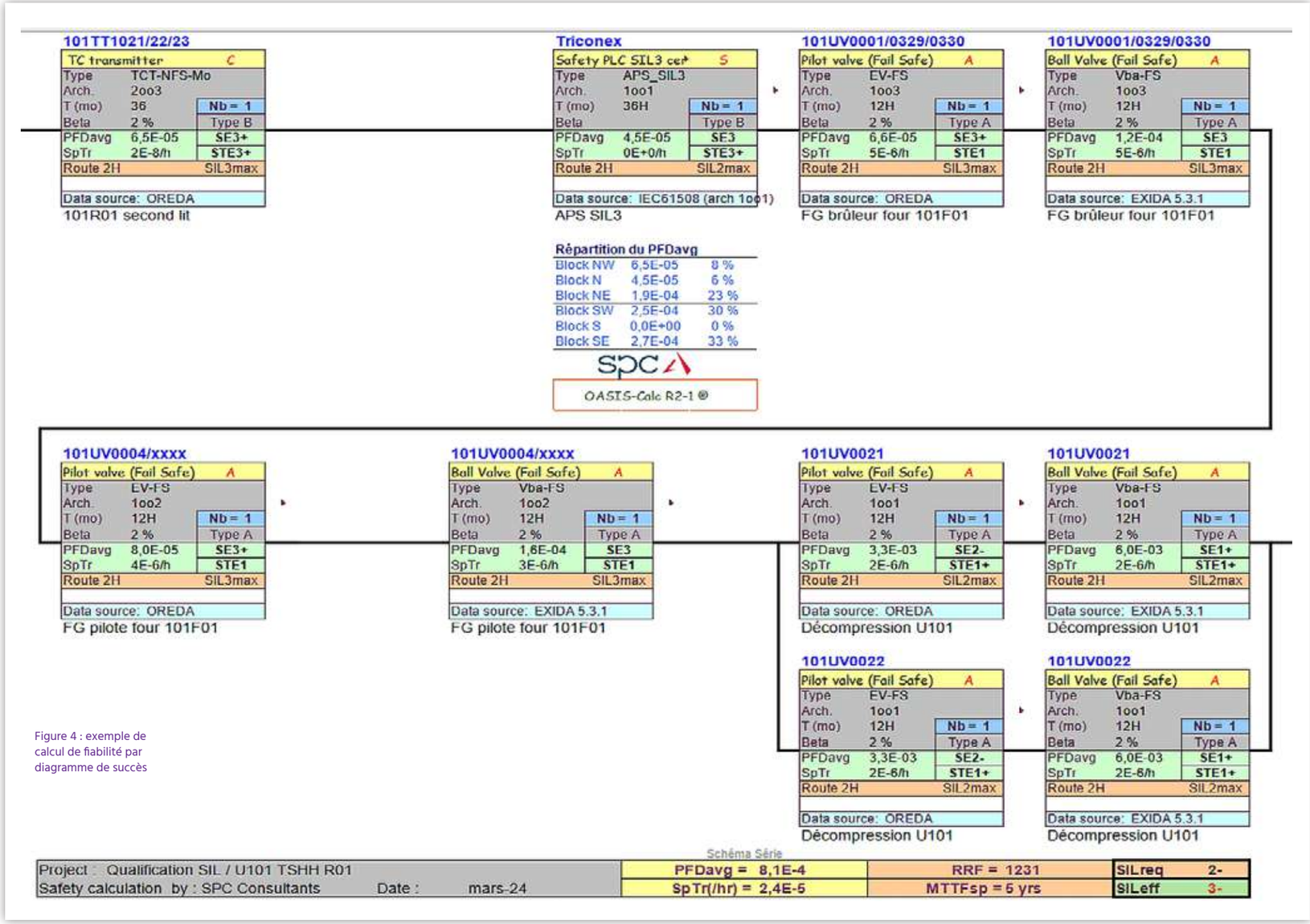

Figure 4 : exemple de calcul de fiabilité par diagramme de succès

SIF_Titre	SIF_Desc	FRR requis	SIL	E/A	Gr	Freq soll	SCL	Rév
LSLL 101X03	Sur détection de niveau bas par LT0603 (transmetteur ajouté et surveillé par LT0003), fermeture de la vanne LV0003 par une électrovanne ajoutée	30	1	A	1	3E-02	3,5	R0
Arrêt d'urgence unité U100	Sur commande opérateur en salle de contrôle ou sur site, arrêt des pompes de transfert du GO L 85P03A/B	10	1-	A	2	1E-04	2,0	R0
LSHH 101B01	Sur détection de niveau haut par LT0601 surveillé par LT0001, fermeture de la vanne LV0001A et LV0001B	30	1	E	1	3E-02	3,5	R0
FSLL asp 101P01A/B	Sur détection de débit bas par FT0714/0605 (surveillés par FT0114/0005), arrêt des pompes 101PT01A/B (une en service arrêt par vanne VH UV0006A et UV0006B)	30	1	E	3	1E-04	2,7	R0
LSLL 101B01 asp 101P01A/B	Sur détection de niveau bas par LT0601 (surveillé par LT0001), arrêt des pompes 101PT01A/B (une en service arrêt par vanne VH UV0006A et UV0006B)	30	1	A	3	3E-07	0,2	R0
FSLL reft 101P01A/B	Sur détection de débit bas par FT0606 surveillé par FT0006, fermeture de la vanne FV0006	10	1-	E	3	1E-04	2,7	R0
BSL four 101F01	Sur détection de perte de flamme par BSLxxxx (un nouveau détectaflamme par bruleur), repli des vannes de bloc gaz UV0001/UV0329/UV0330 pour le FG principal, des vannes gaz pilote UV0004 et UVxxxx (ajoutée)	100	2-	A	3	1E-02	4,7	R0
PSHH FG F01	Sur détection de pression haute FG entrée bruleur par PT0611 surveillé par PT0011, repli des vannes de bloc gaz UV0001/UV0329/UV0330 pour le FG principal	30	1	A	3	3E-05	2,2	R0

Figure 5 : exemple de fonctions de sécurité avec SIL et SCL