Sûreté de Fonctionnement : Normes SIL

La sûreté de fonctionnement est définie par l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage dû au matériel ou à l'environnement. Une analyse des risques permet de déterminer comment la sûreté de fonctionnement permettra d'assurer une protection adéquate contre chacun des risques qui peut survenir. Ces dangers sont donc traités de manière appropriée pendant la phase de conception pour que le système final soit exempt de défaut.

En effet, les fonctions de sécurité sont la résultante des systèmes électriques, électroniques ou électroniques programmables qui sont habituellement complexes, ce qui a pour conséquence de rendre très difficile la détermination des défaillances. L'objectif est donc de concevoir le système d'une manière qui évite un maximum de pannes et qui les contrôle si elles apparaissent.

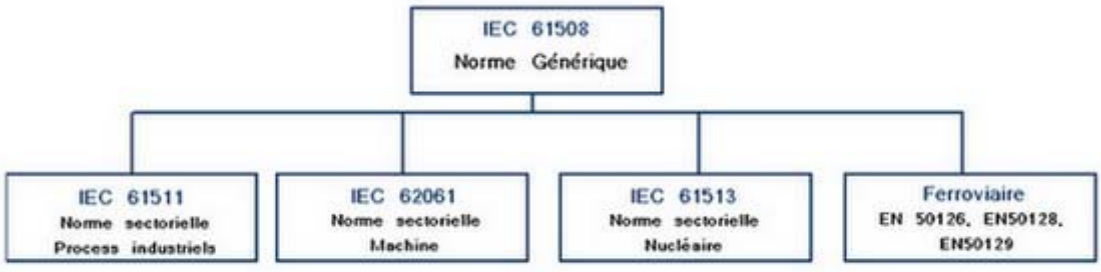
Les pannes peuvent provenir de nombreux facteurs différents :

- Erreurs sur le logiciel,
- Erreur humaine,
- Influence de l'environnement,
- Panne matérielle aléatoire des mécanismes,
- Etc…

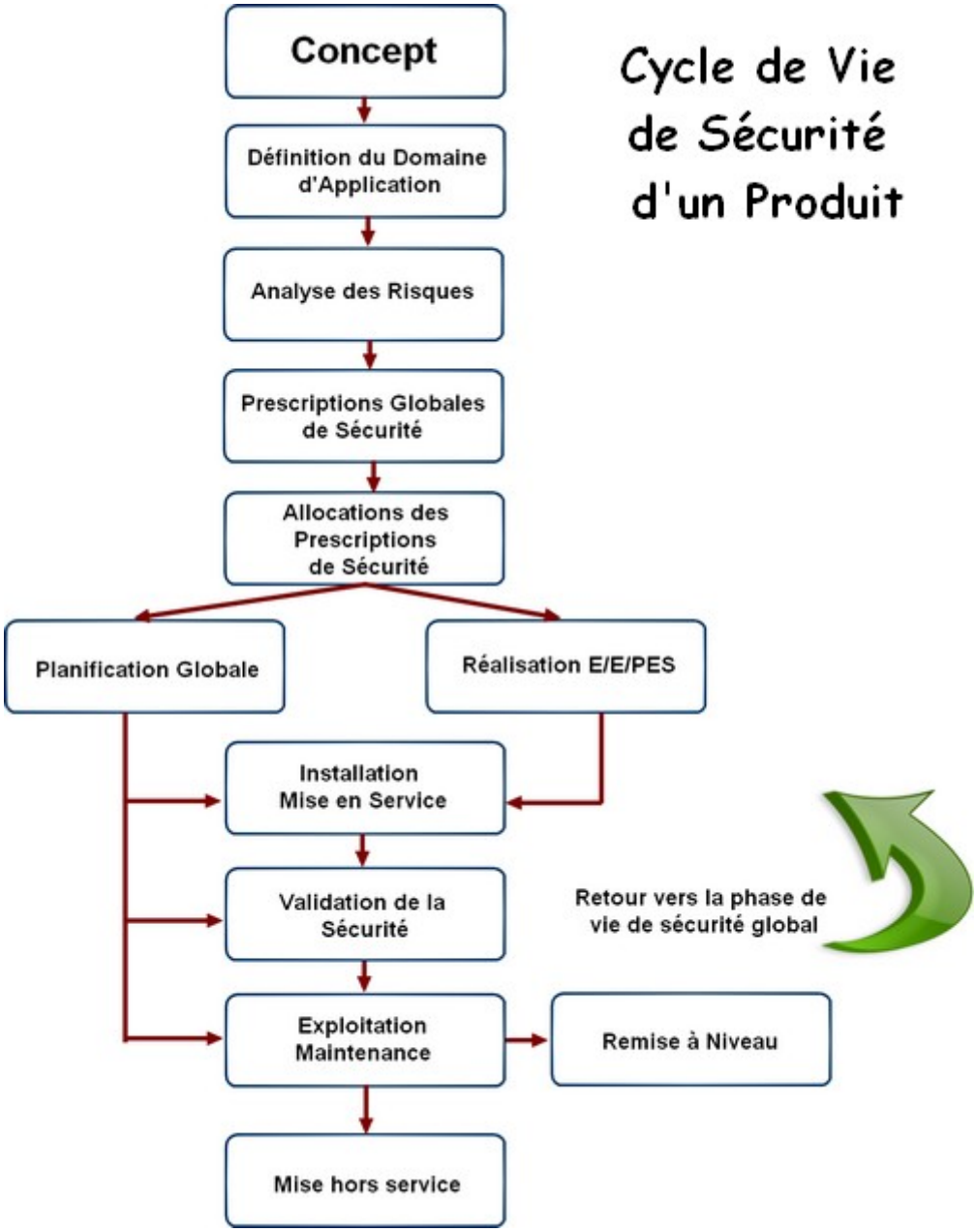
Ainsi, la sécurité de fonctionnement dépend du bon fonctionnement d'un système global ou d'un équipement en réponse à ses entrées.

C'est pourquoi la norme IEC 61508 fut crée. Elle contient les exigences nécessaires et suffisantes pour minimiser ces pannes. Toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service) sont concernées.

L'IEC 61508 a été approuvée par le CENELEC en tant que norme européenne (EN).



Source : Functional Safety and IEC 61508 A basic guide November 2002 : BSI



La norme IEC 61508 présente une approche générique de toutes les activités liées au cycle de vie (naissance jusqu'à la reforme du système) des éléments électriques-électroniques-électroniques programmables (E/E/PES) qui sont utilisés pour réaliser des fonctions de sécurité.

Du fait de la grande variété des applications électriques-électroniques-programmables à des degrés de complexité très divers, la norme IEC 61508 définie des méthodes d'analyse, des méthodes de développement pour réaliser la sécurité fonctionnelle basée sur l'analyse des risques et de déterminer les niveaux d’intégrité de sécurité (SIL) à atteindre pour un risque donné, mais pas de règles générales à proprement dites.

Le SIL ou Security Integrity Level est un niveau d’intégrité de sécurité. La notion de SIL découle directement de la norme IEC 61508. Le SIL peut se définir comme une mesure de la sûreté de fonctionnement qui permet de déterminer les recommandations concernant l'intégrité des fonctions de sécurité à assigner aux systèmes E/E/PE concernant la sécurité.

Il existe 4 niveaux de SIL: le SIL4 étant le système de sécurité le plus élevée.

Il s’agit d’une probabilité moyenne de défaillance sur sollicitation PFDavg (Probability of Failure on Demand) sur une période de 10 ans.

SIL4	Conséquence très importante sur la communauté entraînant une réduction du danger de 10 000 à 100 000.
SIL3	Conséquence très importante sur la communauté et les employés entraînant une réduction du danger de 1 000 à 10 000
SIL2	Protection importante de l'installation, de la production et des employés entraînant une réduction du danger de 100 à 1000.
SIL1	Faible protection de l'installation, de la production entraînant une réduction du danger de 10 à 100.

Grâce à une grande maîtrise en calcul formel, en sécurité de fonctionnement et à l’utilisation de la méthode B (beaucoup utilisée en milieu industriel pour réaliser des logiciels sécuritaires prouvés), ClearSy System Engineering est qualifiée pour mener à bien des projets nécessitants un contexte de certification de niveau SIL 2, SIL 3, SIL 4 selon la norme 61508.