Méthodologie d'évaluation de la sécurité des systèmes automatisés industriels

Philippe Villeneuve de Janti

METHODOLOGIE D'EVALUATION DE LA SECURITE DES SYSTEMES AUTOMATISES INDUSTRIELS

Philippe VILLENEUVE de JANTI
INERIS

Journée de présentation des résultats INERIS à CdF, Hombourg-Haut, 2 juin 1994

1 - INTRODUCTION

De plus en plus, l'industrie électronique recourt à l'évaluation par tierce partie pour améliorer la fiabilité des systèmes et la sécurité des personnels qui les utilisent. Pour faire face à cette demande, l'INERIS a crée le LSSE, Laboratoire de Sécurité des Systèmes Electroniques. Ce Laboratoire permet la mise en commun des moyens et des compétences de l'INERIS et de TECHNICATOME dans le cadre d'un partenariat. Il propose aux entreprises des évaluations de la sûreté de fonctionnement de leurs produits. En aval, en cas d'incident, il expertise et analyse les causes directes et indirectes. Enfin, il délivre une attestation de conformité aux systèmes électroniques, présentés par une entreprise, qui répondent aux exigences de performances, de sécurité et de qualité définies par un cahier des charges.

Deux points sont abordés dans l'exposé :

- le premier, pour présenter la méthodologie d'évaluation de la sûreté de fonctionnement de systèmes automatisés,

- le deuxième, sur le fonctionnement de la procédure de délivrance de certificat qui découle des évaluations effectuées sur les systèmes.

2 - METHODOLOGIE D'EVALUATION DE SYSTEMES AUTOMATISES INDUSTRIELS

L'évaluation de systèmes automatisés industriels ayant des contraintes de sécurité, comporte trois phases, à savoir :

1. l'élaboration du référentiel d'évaluation,

2. l'évaluation fonctionnelle et de type,

3. l'évaluation des actions opérateurs.

2.1 - Elaboration du référentiel d'évaluation

Il n'existe pas dans l'absolu de "bon" ou de "mauvais" système. Le système doit être défini dans les fonctions qu'il doit réaliser et dans l'environnement d'utilisation au sens large. C'est pourquoi, il faut bâtir avant toute action le référentiel d'évaluation. Les éléments de base de sa rédaction sont la procédure d'évaluation et de classification du risque LSSE-92.02 qui intègre le projet de norme EN 954-1, et le dossier technique fourni par le constructeur.

Il comporte les points suivants :

1. Définition du système et ses limites :

- environnement,
- caractéristiques de fonctionnement,
- conditions d'utilisation,
- actions d'un opérateur,
- fonctions à réaliser,
- limites du système étudié (en particulier au niveau de la prise d'information et des actionneurs),
- phase de vie,...

2. Analyse préliminaire des risques.

Cette analyse sommaire est réalisée selon les éléments du dossier technique fourni par le constructeur, en tenant compte des agressions possibles de l'environnement. Elle permet de définir les principales fonctions sur lesquelles pèsent des contraintes de sécurité, ainsi que les événements redoutés. Il s'agit généralement d'événements du type :

- génération d'un ordre intempestif,
- non génération d'une alerte,
- commandes de sécurité non opérationnelles à la sollicitation ...

3. Définition des exigences de sécurité du système.

Les travaux précédents permettent alors de fixer les exigences de sécurité pesant sur le système. Selon le domaine d'utilisation, les conséquences ou effets peuvent être des incidents ou des accidents entraînant des dommages :

- humains,
- économiques,
- environnementaux.

L'analyse préliminaire des risques permet à ce niveau de se fixer des exigences raisonnables en fonction de la gravité des risques.

2.2 - Evaluation fonctionnelle et de type

2.2.1 - Principes

Il est bien évident qu'avant de s'intéresser aux caractéristiques de sécurité d'un système, il faut s'assurer que celui-ci est satisfaisant sur les critères suivants :

- conformité fonctionnelle,
- comportement vis-à-vis des agressions de l'environnement.

L'obtention de cette confiance se fait au travers d'évaluations menées en tierce partie, ou s'appuyant sur des validations/essais menés par le constructeur ou l'utilisateur.

2.2.2 - Essais fonctionnels

Ces essais visent à valider des fonctions de l'équipement par rapport aux performances annoncées dans la documentation technique.

2.2.3 - Essais d'environnement

Les principaux éléments suivants :

- vibrations,
- humidité,
- température,
- poussières,
- ambiance chimique,
- variations de la tension d'alimentation,
- perturbations électriques conduites ou rayonnées,

exercent une action directe sur le niveau de fiabilité et de sécurité des automates programmables. Ces essais visent donc à valider le bon fonctionnement du matériel vis-à-vis des contraintes d'environnement auxquelles ce dernier est susceptible d'être confronté.

2.3 - Evaluation des critères SdF

2.3.1 - Méthodologie

Selon le niveau de sévérité déterminé par le référentiel d'évaluation, l'analyse prend en compte les éléments définis par les étapes suivantes :

Etape 1 - Analyse fonctionnelle et de risque

- Réalisation d'une analyse fonctionnelle.
- Détermination d'une typologie des risques, hiérarchisation des risques suivant le type d'exigence.
- Réalisation d'une analyse des risques.
- Identification des risques envisageables.
- Événements indésirables à analyser.

L'analyse permet de préciser les principales fonctions du système et leurs enchaînements. Après le premier niveau de spécification fonctionnelle, les fonctions principales et contraintes, comme celles liées à la sécurité avec leurs performances associées, sont précisées.

Etape 2 - Analyse de l'architecture

La structure matérielle et logicielle mise en oeuvre est étudiée au regard des exigences de sécurité et de fiabilité déterminées précédemment. L'étude s'appuie sur l'analyse des conséquences des modes de défaillance potentiels des fonctions principales et de contraintes et sur l'évaluation de l'acceptabilité de ces conséquences.

Parmi les solutions habituellement proposées par les industriels, on peut citer :

- redondance active, passive, homogène ou hétérogène,
- traitement temporel déphasé (inhibition du mode commun de défaillance sur perturbations),
- durcissement des auto tests et auto-contrôles,
- langage de programmation structuré,
- utilisation de composants de haute qualité,
- tolérance aux fautes avec voteur n sur m, avec comparateur,...

Chacune de ces solutions a ses avantages et ses limites. Il n'y a pas de "bonne" solution dans l'absolu. C'est pourquoi cette étude est toujours menée au regard du référentiel d'évaluation.

Cette étude est réalisée sur les différents éléments intervenant dans la fonction de sécurité :

- l'unité centrale,
- les interfaces d'entrée et de sortie,
- les capteurs et les actionneurs.

Il est important de noter que les éléments les plus sensibles concernent les interfaces d'entrée et de sortie, ainsi que les éléments externes à l'unité de traitement. En conséquence, une évaluation système est indispensable, qui prend en compte les conditions d'environnement auxquelles sont soumises les fonctions de sécurité.

Etape 3 - Analyse qualitative des modes de défaillance

- Analyse des modes de défaillance et de leurs effets (AMDE).
- Arbres de défaillance.
- Gestion des risques résiduels.
- Analyse qualitative du logiciel.

Cette troisième étape est réalisée sur l'ensemble de la "chaîne" réalisant la fonction de sécurité.

Etape 4 - Analyse quantitative des modes de défaillance

- Evaluation chiffrée des risques résiduels.
- Evaluation du taux de défaillance élémentaire.
- Evaluation des probabilités d'occurrence des événements indésirables.

2.3.2 - Evaluations spécifiques

L'évaluation menée dans les étapes 4 et 5 peut conduire à la réalisation d'évaluations ou d'essais spécifiques tels que :

- évaluation de la qualité logiciel,
- évaluation du comportement sur défaut interne.

2.3.3 - Analyse du logiciel ou des circuits spécialisés

Elle a pour objet d'évaluer la qualité du produit logiciel au travers :

- des structures de développement/suivi mises en place,
- d'évaluations statiques des codes,
- d'analyse des techniques d'auto-test mises en oeuvre.

De même, lorsqu'il est fait appel à des composants intégrant toujours davantage de fonctions, tels que les ASIC, PAL, Gate Array programmable, les structures de développement et de validation sont analysées.

2.3.4 - Analyse du comportement sur défaut interne

Une défaillance interne a pour origine la défaillance d'un composant, la rupture d'une piste ou d'une connexion, ou tout type de court-circuit entre conducteurs.

Cette analyse portera donc sur la capacité à détecter des dysfonctionnements internes par les auto tests et les tests périodiques.

Les techniques mises en oeuvre comportent des analyses de schémas électriques et des injections physiques de défaillance sur la configuration test.

Les modèles de fautes sont généralement :

- défauts de connexion : ouverture de contact , débrochage de cartes, coupures de liaisons,
- défauts de composant : forçage à 0 ou 1, ou coupure des broches de composants (intégrés ou discrets),
- défauts sur unité centrale : injection d'erreurs dans le programme par "émulation de la mémoire" en utilisant des outils de test adaptés.

2.4 - Evaluation des actions de l'opérateur

Dès que les fonctions assurées par un système ne sont plus très simples, l'influence d'un opérateur de conduite ou de maintenance peut venir mettre en défaut les dispositions de sécurité mises en place.

Il n'existe hélas pas de technique pour assurer à coup sûr qu'un opérateur ne fera pas d'erreurs, tous les incidents connus sont là pour le prouver. On peut cependant limiter largement ce risque, par une bonne prise en compte de ses interventions lors de la conception :

- qualité des signalisations,
- dispositions constructives interdisant certaines actions,
- qualité des techniques de test,
- qualité des documentations, ...

Des techniques d'analyse de ces dispositions peuvent être mises en oeuvre pour évaluer la "qualité" globale de l'interface homme/machine.

2.5 - Synthèse

L'évaluation sûreté de fonctionnement d'un système fait appel à une démarche **globale** utilisant des techniques diverses et complémentaires.

La profondeur d'analyse, donc son coût, doit être en rapport avec le niveau de contrainte du système.

Il n'y a pas **une** solution pour obtenir la sécurité.

Il n'y a pas **une** technique pour évaluer la sécurité.

3 - FONCTIONNEMENT DE LA PROCEDURE DE DELIVRANCE D'ATTESTATION

3.1 - Champ d'application

L'attestation concerne les systèmes électroniques à usage industriel :

- susceptibles d'entraîner des risques par eux-mêmes, par l'usage qui en est fait, ou utilisés dans des environnements à risques,
- dont la vocation est de prévenir ces risques (ayant une fonction de sécurité).

Les principaux domaines d'application couverts par l'attestation sont :

- contrôle de procédé en chimie,
- contrôle de procédé dans le domaine agro-alimentaire,
- contrôle de procédé en métallurgie,
- contrôle de procédé en production d'énergie,...
- robots, contrôleurs, automates programmables industriels ayant des fonctions de sécurité,
- télécommandes industrielles,
- systèmes électroniques embarqués sur des engins mobiles,
- dispositifs de télésurveillance.

3.2 - Définition de l'attestation de conformité

L'attestation de conformité atteste, à partir d'examens et de tests réalisés en laboratoire, que les systèmes sont conformes aux exigences définies dans un cahier des charges.

Il est destiné aux industriels désireux d'intégrer un haut niveau de sécurité dans leurs produits et de valoriser ainsi leur savoir-faire technique.

3.3 - Déroulement de la procédure

La procédure comporte quatre étapes :

- une étude initiale : qui sert à recenser les fonctions les plus critiques, les risques potentiels et les fonctionnalités du système pouvant prévenir ces risques.

Il est établi ensuite un dossier relatif à la Sûreté de Fonctionnement (SdF) et un programme d'évaluation et contrôle constituant **le cahier des charges** auquel devra satisfaire le système à évaluer. Il est réalisé soit sur un produit fini, soit dès la conception du produit.

- une phase d'évaluation. Les types d'évaluation auxquels il est recouru peuvent se faire en application d'une norme. Dans d'autres cas, les spécialistes du LSSE déterminent et caractérisent les évaluations nécessaires en fonction de l'analyse du dossier d'étude initiale et de leur propre expérience.

Certains tests déjà réalisés par le demandeur peuvent être pris en compte s'ils sont conformes à la méthodologie prédéfinie par le LSSE.

- une étape d'attribution de "l'attestation LSSE", après avis de la commission d'attribution.

- une phase de suivi des systèmes couverts par l'attestation, sous forme d'audits.

3.4 - Bases scientifiques

Les bases scientifiques sur lesquelles s'appuie la procédure d'évaluation sont les normes et connaissances disponibles qui ont été développées en France, ainsi qu'à l'étranger.

Les règlements techniques, élaborés par catégorie de produits, précisent les différentes spécifications techniques applicables lorsqu'il n'existe pas de documents normatifs.

3.5 - Règlement technique

Les Règlements Techniques sont établis pour les matériels propres à une catégorie de produit (télécommandes industrielles,...). Ils sont élaborés par les experts du LSSE, puis soumis pour avis et commentaires à un groupe de travail ad hoc composé de représentants des utilisateurs et des fabricants.

Le Règlement Technique précise les différentes spécifications techniques applicables. Il s'appuie sur la normalisation déjà existante en Europe sur la question - et en particulier - sur le projet de norme EN 954-1.

Il définit en particulier :

- la catégorie de produits concernée et les limites de cette catégorie,
- les critères retenus en matière de sécurité,
- les exigences et valeurs limites acceptables retenues lorsqu'il est établi qu'une quantification en la matière trouve des fondements scientifiques ou qu'il existe des documents normatifs.

Dans le cas où des critères ne peuvent être assortis de valeurs limites, chaque Règlement Technique précise :

- les modalités d'évaluation des caractéristiques correspondantes du produit et de prise de décision pour l'attribution de l'attestation,
- les méthodes d'évaluation retenues pour mesurer l'impact du produit sur la sécurité et l'environnement, et donc démontrer la conformité du produit aux spécifications retenues, qu'elles soient de nature qualitative ou quantitative,

- les normes ou spécifications que le produit doit respecter en matière d'aptitude à l'usage, de sécurité,...

Pour certains matériels, une concertation avec l'ensemble des parties concernées peut s'engager préalablement à toute élaboration d'un règlement technique par le LSSE .

Citons le cas des automates programmables industriels où un consensus se dégage pour lancer des travaux de réflexion sur les méthodologies d'évaluation à mettre en oeuvre dans le cadre d'un groupe ad hoc réunissant des constructeurs d'équipements d'informatique industriels, des ensembliers, des organismes d'étude sur la sécurité et le GIMELEC.

3.6 - Cahier des charges

Il est spécifique à chaque produit. Il nécessite une étude initiale conduite sur la base des informations transmises par le demandeur.

Avec un diagnostic sur la probabilité d'attribution de l'attestation LSSE, il comportera :

- la liste et la description des évaluations, essais et contrôles à effectuer et des résultats à obtenir,
- le nombre de pièces à fournir au LSSE et le mode de prélèvement s'il y a lieu,
- les modalités spécifiques éventuelles de l'évaluation de la conformité des produits certifiés.

3.7 - Délivrance de l'attestation de conformité

Les procédures d'essais mises en oeuvre, les résultats issus de l'analyse sûreté de fonctionnement et des essais, ainsi que leur interprétation font l'objet d'un rapport d'évaluation.

Si les spécifications décrites dans le cahier des charges ont été atteintes lors de l'évaluation, l'attribution de l'attestation de conformité selon la classe d'exigence définie sera effectuée.

Dans le cas contraire, des recommandations à l'attention du constructeur, lui permettant d'améliorer son matériel, sont effectuées.