LES AUTOMATES PROGRAMMABLES INDUSTRIELS DANS L'ANALYSE DE RISQUE DES ETUDES DE DANGER

PROGRAMMABLE LOGIC CONTROLLERS IN DAM SAFETY ANALYSIS

Dominique RIOUAL
EDF Centre d'Ingénierie Hydraulique
Savoie Technolac – 4 allée du Lac de Tignes 73290 La Motte Servolex - France
dominique.rioual@edf.fr

MOTS CLEFS

Contrôle-commande, automate programmable industriel, analyse de risque, Etude de Danger, défaillance, dysfonctionnement.

KEY WORDS

Control system, programmable logic controller, PLC, risk analysis, Safety analysis, fault

RÉSUMÉ

Les systèmes de contrôle-commande des barrages bénéficient des évolutions technologiques récentes en intégrant davantage d'équipements numériques et d'automates programmables. Ceci permet de répondre à des besoins d'automatisation accrus, et contribue à la sûreté de l'ouvrage.

EDF Hydro a récemment intégré ces évolutions dans le référentiel technique de contrôle-commande de ses barrages. Ce nouveau système est en cours de déploiement sur le parc. La nouvelle architecture a conduit le Centre d'Ingénierie Hydraulique d'EDF à revoir les principes de cotation des automates programmables dans l'analyse de risque de l'EDD.

Cet article présente dans les grandes lignes les principes méthodologiques retenus, qui permettent de clarifier les modes de défaillance et d'obtenir une cotation reflétant mieux la réalité des automatismes présents sur l'ouvrage.

La méthodologie, centrée sur l'automate, contribue également à avoir une meilleure vision du parc d'automates en exploitation, contribuant ainsi à la sûreté des ouvrages exploités par EDF Hydro.

ABSTRACT

Dam control systems benefit from recent technological developments, with more digital equipment and programmable logic controllers. This makes possible to meet new needs, such as an increase in the level of automation, and contributes to the safety of the dam.

EDF Hydro has recently integrated these developments into its dam control system. The new system is currently being deployed across the fleet. The new architecture has led EDF Hydro Engineering Centre to review the principles of PLC rating in the EDD risk analysis.

This article outlines the methodological principles adopted, which clarify the failure modes and give a rating that reflects more accurately the state of the control systems in operation on site.

The methodology, which focuses on the PLC, also helps to have a better overview of the fleet of PLCs in operation, thus contributing to the safety of the dam operated by EDF Hydro.

1. INTRODUCTION

Les systèmes de contrôle-commande font l'objet d'évolutions technologiques permanentes et la tendance est d'intégrer davantage de systèmes numériques. Les contrôles-commandes des barrages n'y font pas exception. Les besoins d'exploitation évoluent également, avec un degré d'automatisation accrus, l'aide aux exploitants des barrages, et l'exigence de toujours améliorer la fiabilité et de la sûreté.

EDF Hydro a intégré ces besoins en faisant évoluer son référentiel technique de contrôle-commande. Ce nouveau système, en cours de déploiement, s'appuie sur une architecture avec plusieurs automates programmables industriels sur lesquels se répartissent les fonctions nécessaires à la conduite et à la sécurisation de l'ouvrage.

Ceci a également conduit EDF Hydro à se requestionner sur l'impact des automates dans l'analyse de risques des EDD, et notamment comment objectiver les améliorations fonctionnelles et techniques apportées par le nouveau référentiel.

EDF CIH a ainsi revu la méthodologie de cotation des automates dans l'analyse de risques de l'EDD. Les principes retenus sont abordés dans cet articles.

2. PRESENTATION GENERALE DU CONTROLE-COMMANDE DU BARRAGE

Les fonctions assurées par le contrôle-commande dépendent fortement de la configuration du barrage ; un barrage peut être très simple du point de vue du contrôle-commande, en fonction de la présence ou non de vannes motorisées et du degré d'automatisation requis. Les contrôles-commandes complexes portent des fonctions de conduite automatique qui permettent d'assurer la tenue du plan d'eau en l'absence d'exploitant sur l'ouvrage (cas des BMR par exemple). Dans le cas d'ouvrages non vannés, il peut ne pas y avoir d'automate présent au barrage ou alors l'automate assure des fonctions très simples comme l'acquisition des mesures de niveaux.

Dans le cas d'un barrage complexe avec des vannes motorisées et une conduite automatique, les fonctions portées par le contrôle-commande sont les suivantes :

Fonction	**Périmètre**	**Equipements**
Fonctions de surveillance et de commande	Supervision locale au barrage ou à distance Alarmes.	Poste de conduite centralisé sous la forme d'une IHM numérique. Serveur de données temps réel. Réseau local industriel de l'ouvrage. Chaîne de détection, de transmission et diffusion des alarmes.
Fonctions de conduite du barrage	Conduite automatique du barrage assurant une régulation de niveau ou de débit et la commande automatique des vannes EVC.	Automate de conduite du barrage
Fonction de sauvegarde	Dispositif de sauvegarde déclenchant l'ouverture des vannes sur atteinte d'un niveau critique.	Automate de sûreté
Fonctions de gestion et de manœuvre de la vanne ou de la passe.	Commande de manœuvre de la vanne ou de la passe Protections de la vanne.	Automate de Passe Contrôle-commande de 1er rang à relais Dispositif Temps Trop Long
Fonctions de mesure et détection	Instrumentation.	Capteurs de position Capteur de niveau Fins de course
Alimentations électriques	Alimentation nominale du barrage et alimentation de secours.	Auxiliaires du barrage Groupe Electrogène de secours

Ces fonctions sont architecturées suivant plusieurs niveaux ou rangs :

- Le rang 0 correspond au process physique (vannes, passes) en interface du contrôle-commande.
- Le rang 1 est la partie du contrôle-commande en interface directe avec le process, son périmètre est celui de la vanne ou de la passe. Il est constitué de capteurs, de relayage et d'un automate de passe.
- Le rang 2 constitue le contrôle-commande dont le périmètre d'action est le barrage. Il est essentiellement constitué :
    - D'un automate de conduite qui assure la régulation du niveau ou du débit de l'ouvrage, la répartition des débits sur les différentes vannes ou passes qu'il commande
    - Du dispositif de sauvegarde matérialisé par l'automate de sauvegarde.
    - D'un serveur informatique centralisant les données du barrage et d'une interface homme-machine permettant la surveillance et la commande centralisée par l'exploitant. Ce serveur met à disposition les données au système de supervision à distance (hors site) de rang 3.
- Le rang 3 est un système de supervision « hors site » permet d'accéder aux données de l'ouvrage à distance.

Il est à noter que de nombreux systèmes de contrôle-commande déployés dans les dernières décennies sur les barrages d'EDF Hydro sont basés sur des technologies plus anciennes qui utilisent du relayage pour les fonctions de 1er rang et le dispositif de sauvegarde.

3. LES AUTOMATES DANS L'ANALYSE DE RISQUE

La méthodologie de cotation retenue par EDF CIH permet d'analyser l'ensemble des systèmes de contrôle-commande, quelle que soit leur génération. Néanmoins, les exemples donnés dans cet article correspondent au dernier référentiel technique d'EDF Hydro, où l'essentiel des fonctions sont portées par des automates programmables industriels.

3.1 Risques et opportunités de l'automate programmable

Les fonctions portées par les automates contribuent à la sûreté de l'ouvrage. En effet, elles permettent d'assurer le maintien du barrage dans sa zone d'exploitation nominale lorsque l'exploitant n'est pas sur site, assurent la conduite automatique de l'ouvrage, permettent une surveillance de l'ouvrage à distance, et évitent un exhaussement dangereux du niveau amont.

Puisqu'un certain nombre de tâches anciennement assurées par l'exploitant sont désormais confiées à l'automate, ce dernier devient particulièrement critique et toute défaillance a des conséquences sur la sûreté du barrage. Ces défaillances sont donc présentes dans l'analyse de risque de l'EDD.

Les automates de conduite et de sûreté peuvent commander une part significative voire la totalité du débit passant par les EVC, et les conséquences de leur défaillance potentielle sur le risque à l'amont et à l'aval du barrage sont importantes.

3.2 Les modes de défaillance

Il est important clarifier les deux modes de défaillance d'un automate qui sont de nature et de probabilité différentes. Les deux modes considérés sont :

- Le non-fonctionnement, similaire à une panne : l'automate n'agit pas alors qu'il devrait. Ceci peut être causé par une panne matérielle ou une perte d'alimentation de l'automate. Le non-fonctionnement correspond également à un mode de repli lorsque l'automate détecte une anomalie critique et qu'il ne peut plus conduire le barrage (perte de la mesure de niveau par exemple).
- Le dysfonctionnement : l'automate agit mais de façon non conforme à l'attendu. Par exemple, il commande l'ouverture des vannes du barrage au-delà du débit souhaité ce qui entraine un sur-débit à l'aval. L'anomalie logicielle ou un fonctionnel inadapté font partie des causes de dysfonctionnement.

4. L'AUTOMATE DANS LES SCENARIOS DE DEFAILLANCE

L'analyse de risque menée par EDF dans le cadre de l'EDD consiste à établir des scénarios de défaillance pouvant conduire à des événements indésirables dénommés **Événement Redoutés Centraux** (ERC), parmi lesquels : rupture du barrage, rupture d'une vanne, ouverture intempestive d'une vanne, ouverture intempestive de l'ensemble des vannes du barrage.

Les scénarios de défaillances et de conséquences sont modélisés sous la forme de « nœuds papillon » qui représentent :

- Les événements initiateurs (EI) à l'origine de la défaillance et les éventuelles barrières de prévention permettant de limiter la probabilité d'apparition de l'ERC.
- Les conséquences de l'ERC et les éventuelles barrières de protection pouvant limiter les effets.

Ces scénarii sont ensuite probabilisés en utilisant la méthode semi-quantitative développée par l'INERIS.

L'automate intervient dans ces scénarios soit en tant qu'événement initiateur, en cas de défaillance, soit en tant que barrière.

4.1 Les scénarios de défaillance étudiés dans l'EDD

Ils sont de natures (mode de défaillance) et de périmètres différents. Le tableau ci-après recense les principaux scénarios associés aux modes de défaillance et aux périmètres considérés ; soit une seule vanne, soit l'ensemble – ou une part importante – des vannes de l'ouvrage.

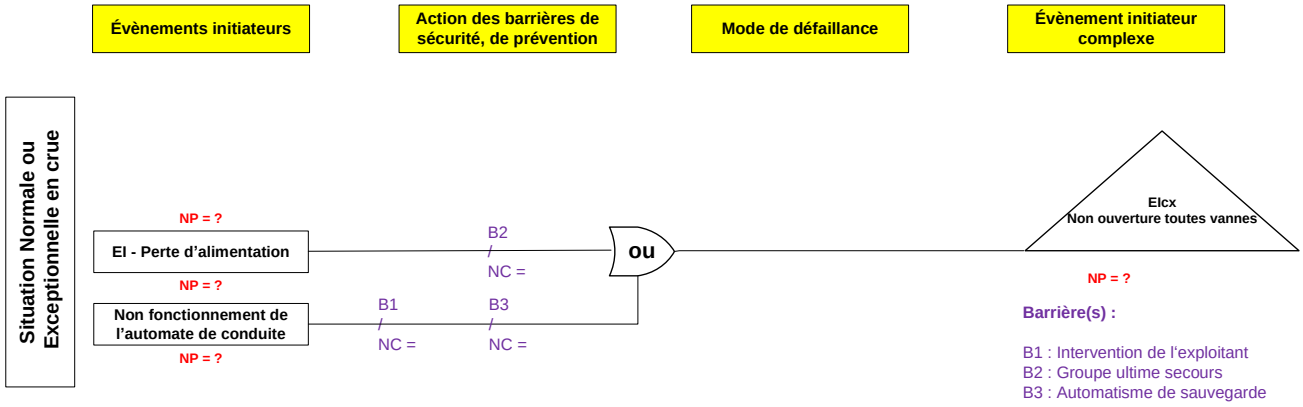
Mode de défaillance	**Une seule vanne**	**Ensemble des vannes**
Non-Fonctionnement	Non-ouverture d'une seule vanne	Non-ouverture du barrage
Dysfonctionnement	Ouverture intempestive d'une seule vanne	Ouverture intempestive du barrage
	+ Fermeture intempestive une seule vanne	Fermeture intempestive du barrage

L'approche d'EDF CIH a été de faire pour chaque scénario une analyse des modes de défaillance du système de contrôle-commande formalisée ensuite par les nœuds-papillon de l'EDD.

4.2 Exemples de scénarii

Scénario de non-ouverture de l'ensemble des vannes

Le scénario de non-ouverture de l'ensemble des vannes est un EI complexe qui peut conduire à l'exhaussement de niveau amont du barrage, entraînant la rupture de l'ouvrage (ERC « rupture barrage ») si le niveau dépasse une cote critique.



Nœud-papillon du scénario « non-ouverture toutes vannes »

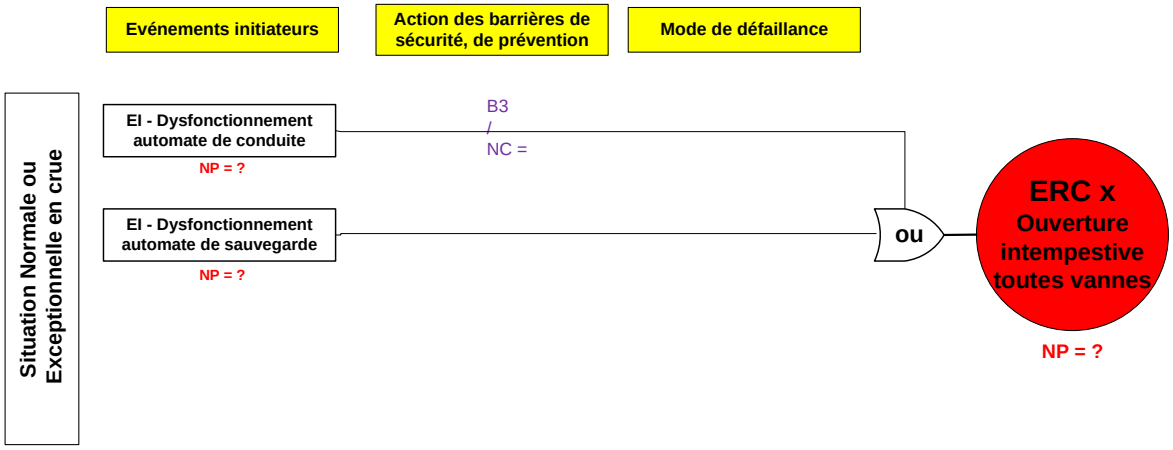
Les automates intervenant dans ce scénario sont :

- L'automate de conduite en charge de réguler le niveau du barrage ; sa défaillance de non-fonctionnement est un événement initiateur.
- L'automate de sûreté enveloppe faisant partie du dispositif de sauvegarde, qui intervient en tant que barrière de prévention, puisqu'il est capable d'ouvrir les vannes automatiques sur atteinte d'un niveau très haut avant l'atteinte de la cote critique.

L'intervention humaine reste une barrière essentielle, soit pour reprendre la conduite en manuel sur non-fonctionnement de l'automate de conduite, soit pour mettre en œuvre le groupe d'ultime secours en situation de perte d'énergie.

Scénario d'ouverture intempestive de l'ensemble des vannes

Cet ERC concerne le risque à l'aval de l'ouvrage dans une situation où le débit relâché ne serait pas maîtrisé.



Nœud-papillon du scénario « ouverture intempestive toutes vannes »

L'automate de conduite et l'automate de sauvegarde figurent dans le scénario en tant qu'évènements initiateurs. En effet, ils peuvent faire l'objet d'une défaillance de type dysfonctionnement conduisant à ouvrir les vannes. Les barrières de prévention sont très limitées dans ce scénario, le phénomène étant rapide et pouvant se produire en l'absence de l'exploitant. Néanmoins, ce type de phénomène est d'une occurrence bien plus faible que le non-fonctionnement d'un automate.

Il est néanmoins possible de limiter le débit commandable par l'automate de conduite par un moyen externe, par exemple en limitant l'ouverture d'une vanne par un contact de fin de course ou en laissant une partie des vannes hors énergie. Ainsi, ce sont les conséquences du dysfonctionnement qui sont réduites. Ces dispositions seront supprimées lors de la crue afin que l'automate de conduite puisse passer le débit nécessaire.

Cette logique de limitation est plus difficile à mettre en œuvre pour l'automate de sauvegarde qui doit conserver un débit commandable suffisant pour sauvegarder l'ouvrage en cas d'atteinte de niveau extrême.

4.3 Autres barrières de contrôle-commande

D'autres protections de contrôle-commande sont utilisées pour limiter les manœuvres intempestives des EVC et les variations de débit à l'aval. Ces dispositifs usuels sont les suivants :

- Le dispositif de crantage qui garantit une manœuvre par pas,
- Le contrôle d'un temps maximum de manœuvre,
- Les fins de course limitant l'ouverture à un débit maximum hors crue, le principe étant de laisser un débit commandable à l'automate suffisant pour assurer le report de débit de l'usine. Ce dispositif est désactivé en début de crue. La limitation du débit commandable hors crue peut également se faire en mettant une ou plusieurs vannes hors tension.

Le crantage et le contrôle de temps de manœuvre sont efficaces pour limiter l'ouverture ou la fermeture à la suite d'une défaillance du 1er rang, mais ne le sont pas face à un automate dysfonctionnel.

La barrière « intervention de l'exploitant » reste essentielle pour qu'il puisse reprendre le contrôle de son barrage en cas de défaillance du système de contrôle-commande.

5. COTATION DES DEFAILLANCE DES AUTOMATES PROGRAMMABLES

5.1 Un exercice complexe

Les cotations d'une défaillance de non-fonctionnement ou de dysfonctionnement de l'automate de conduite ou de l'automate de sauvegarde sont particulièrement délicates. En effet, les causes de défaillances sont multifactorielles. Elles peuvent être externes à l'automate lorsque les données d'entrée sont erronées (notamment les mesures de niveau ou les consignes saisies par l'opérateur), être liée aux fonctions portées par l'automate, à un fonctionnement logiciel non souhaité ou non anticipé s'exprimant uniquement dans des conditions rares, à une erreur de paramétrage ou à une panne matérielle.

Il est également nécessaire de tenir compte de l'hétérogénéité des automates qui s'explique par la diversité des barrages en exploitation et par l'ancienneté des contrôles-commandes. L'on retrouve ainsi une forte diversité technologique avec différents fabricants et gammes d'automates, différentes architectures logicielles, de nombreux langages de programmation, et des fonctions portées par les automates qui ne s'appuient pas toujours sur le référentiel actuel.

Enfin, il convient également de constater que dans l'ensemble de la chaine (conception, déploiement, maintenance) le facteur humain rentre également en ligne de compte. Il est valable tant dans la relation entre l'exploitant et son contrôle commande qu'au niveau du fournisseur et mainteneur.

5.2 Principe de cotation

Le principe est de différencier la cotation en fonction du mode de défaillance ; non-fonctionnement (pas d'action de l'automate alors qu'il aurait dû agir) et dysfonctionnement (l'automate agit mais de façon non conforme à l'attendu).

Le non-fonctionnement est considéré comme plus probable qu'un dysfonctionnement car il peut être causé par une panne matérielle ou une perte d'alimentation de l'automate. Il correspond également à un mode de repli lorsque l'automate détecte une anomalie critique et qu'il n'a plus la possibilité conduire le barrage (perte de la mesure de niveau par exemple).

La cotation de la défaillance de l'automate s'appuie principalement sur le REX interne. En effet, EDF Hydro trace l'ensemble des événements de sûreté liés à l'exploitation ou à l'activité d'ingénierie, ces événements faisant l'objet d'une analyse. D'autres sources d'information sont utilisées : EISH, base ARIA, ou REX d'événements à l'international (ces derniers étant assez rare en ce qui concerne le contrôle-commande).

Nota :

Il existe des normes traitant de la sécurité fonctionnelle de systèmes de sécurité utilisant des technologies électriques/électroniques/programmables, comme l'IEC 61508 ou l'IEC 61511 (systèmes instrumentés de sécurité). Ces normes permettent d'établir un niveau SIL (Safety Integrity Level) pour les fonctions de sécurité de l'automate et de calculer un taux de défaillance absolu.

Cette approche normative n'est pas utilisée dans la méthodologie présentée dans cet article ; EDF utilise une méthodologie semi-quantitative dans l'analyse de risque de l'EDD avec une approche qui reste conservative, en particulier lorsque l'automate constitue une barrière de prévention. Le REX sur les automates de conduite en exploitation montre également une prédominance de dysfonctionnements liés à un fonctionnel non adapté, la quantification de ce type de défaillance restant difficile à établir.

5.3 Cotation du dysfonctionnement

Il est important de comprendre les causes pouvant mener à un dysfonctionnement. Celles-ci sont de natures différentes et peuvent être :

- Externes à l'automate :
  - Une mesure erronée et non détectée par l'automate (niveau amont ou débit entrant)
  - Une consigne saisie par l'opérateur erronée est appliquée par l'automate.

  Il convient alors de vérifier que l'automate prévoit des contrôles qui le rend robuste à des entrées erronées ou invalides. En effet, si un contrôle détecte une perte d'intégrité d'une valeur et l'invalide, il n'y a aura pas de dysfonctionnement de l'automate. La multiplication de ces contrôles, intégrée de façon systématique dans un référentiel technique permet de capitaliser sur le REX et ainsi, d'obtenir une amélioration continue de la sûreté des automates.

- Internes à l'automate :
  - Une anomalie logicielle non détectée lors de la phase de conception ou lors d'une requalification.
  - Mauvais paramétrage.
  - Robustesse du fonctionnement, des contrôles devant être effectués par l'automate pour qu'il puisse détecter que les fonctions de conduite ne sont plus opérationnelles.

La méthodologie pour caractériser la probabilité du dysfonctionnement intègre ces différentes causes et consiste à élaborer un indice de confiance de l'automate en fonction de critères auditables. Ces critères couvrent trois axes :

- L'historique de l'automate qui peut indiquer des défaillances récurrentes non solutionnées ;
- La conception initiale de l'automate ;
- La maintenabilité, qui indique la facilité à maintenir l'automate en condition opérationnelle.

En fonction de l'indice de confiance obtenu, la probabilité de dysfonctionnement est évaluée de courante, jusqu'à improbable, ce dernier cas étant atteint lorsque les critères sont atteints.

Ainsi, la cotation du dysfonctionnement d'un automate dans l'analyse de risque de l'EDD peut évoluer entre A2 et C.

5.4 Focus sur quelques critères de l'indice de confiance

Catégorie	Critère
Historique	• Avis de l'exploitant sur la fiabilité de l'automate sur la base d'un entretien. • Avis du mainteneur sur la fiabilité de l'automate objectivé par les faits techniques observés depuis la mise en service.
Conception	*Conformité du code et règles de développement* • Le code respecte-il les règles de codage du référentiel technique d'EDF Hydro ? • Dispose-t-il d'une structure modulaire ? • Utilise-t-on des modules standards ? *Fonctionnel* • Une étude de conduite a-t-elle été menée sur la base d'une expression de besoin formalisée ? • Comportement de l'automate sur défaut : - L'automate dispose-t-il de protections d'automatisme en conformité avec le référentiel technique d'EDF Hydro ? - L'automate est-il robuste face à des mesures ou des consignes invalides ou dysfonctionnelles ? *Validation* Qualité des tests effectués en plate-forme et sur site lors de la mise en service de l'automate
Maintenabilité	• Les documents techniques associés au programme sont-ils existants et à jour ? La fiche de version est-elle à jour et trace-t-elle les modifications effectuées ? • Testabilité : Un simulateur de partie opérative existe-t-il pour tester cet automate en plate-forme ? • Qualité et complétude de la documentation technique, et traçabilité des modifications • Compétences disponibles en interne sur cet automate

5.5 Une logique de différentiation des impacts du dysfonctionnement

Dans l'analyse de risque, il faut garder à l'esprit que le débit non maîtrisé en cas de dysfonctionnement est limité par le débit commandable par l'automate.

En outre, l'occurrence du dysfonctionnement ne peut être vue indépendamment du débit non maitrisé. En d'autres termes, plus le débit relâché non maîtrisé et important, moins cet événement est probable, et il ne faut pas appliquer l'impact le plus grave à l'occurrence d'ouverture la plus fréquente.

5.6 Cotation du non-fonctionnement

Comme évoqué précédemment, le non-fonctionnement est estimé plus probable que le dysfonctionnement car les causes diffèrent. L'indice de confiance élaboré pour la cotation du dysfonctionnement reste un indicateur pertinent, mais l'occurrence de l'évènement initiateur restera plus élevée, typiquement entre A2 et B.

5.7 Exemple d'application à un barrage localisé dans l'est de la France

Cette méthodologie a été utilisée pour sur l'automate de conduite (APB) d'un barrage situé dans l'est de la France. Le contrôle-commande et l'APB étaient en cours de rénovation lors de la mise à jour de l'EDD.

L'ensemble des critères prévus pour l'établissement de l'indice de confiance ont été examinés (à l'exception de l'historique l'automate étant neuf) ce qui a permis d'obtenir un indice de confiance et une cotation favorable. En effet, l'automate s'appuie sur un référentiel technique récent satisfaisant les critères de codage de d'adéquation du fonctionnel. Une étude de conduite a également été effectuée.

Une analyse complète des contrôles internes implémentés dans l'automate a permis de quantifier le débit maximum relâché non maîtrisé, et de vérifier que cette valeur restait compatible avec l'analyse de risque de l'EDD. Les EI suivants ont été considérés :

- EI « fermeture intempestive d'une ou plusieurs vannes par l'APB » en crue pouvant conduire à l'exhaussement de niveau puis à la rupture du barrage.

- EI « ouverture intempestive d'une ou plusieurs vannes par l'APB » entrainant un risque à l'aval du barrage.

L'analyse a également bénéficié à la qualité finale de l'automate puisqu'elle a produit les recommandations suivantes :

- Concernant les essais, nécessité de constituer un dossier de qualification complet (avec tests plate-forme et site), et nécessité d'effectuer des tests en plate-forme de passage de crues importantes couvrant la plage de fonctionnement de l'automate
- Effectuer une revue de code par un automaticien indépendant de l'équipe de développement
- Conditions de transfert à l'équipe en charge de la maintenance tel que la mise à jour de la simulation et de la documentation technique une fois l'automate en service.
- Mise à niveau du traitement de régulation de niveau pour intégrer les dernières évolutions du référentiel technique.

Ces recommandations ont été respectées par l'équipe de développement, de façon à garantir la cotation des EI en lien avec une défaillance de l'automate.

6. RECOMMANDATIONS SUR LE DEVELOPPEMENT DES AUTOMATES

Les automates de conduite barrage et les automates de sauvegarde doivent faire l'objet d'une attention particulière du fait de la criticité des fonctions qu'ils portent. Au-delà des règles de l'art concernant le développement du logiciel, basé sur un cycle en V et soumis à des procédures de qualifications très strictes, voici quelques points d'attention à considérer lors de la conception.

6.1 L'importance de l'étude fonctionnelle

Une étude fonctionnelle détaillée doit permettre de spécifier les traitements et leurs paramètres, en tenant compte de l'exploitation du barrage. Ceci est particulièrement critique pour les fonctions de conduite tel que la régulation du plan d'eau ou la répartition du débit sur les vannes du barrage.

6.2 La robustesse face aux donnés d'entrée erronées

- Les données acquises par l'automate, que ce soient des consignes saisies par un opérateur ou des mesures acquises sur le process, peuvent à tout moment devenir erronées ou invalides. Il est primordial que l'automate soit capable de détecter les anomalies sur ces données et que les traitements en tiennent compte. Dans le cas où l'automate ne dispose plus des données indispensables pour conduire le barrage, il doit alerter l'exploitant qui reprendra la conduite du barrage en manuel.
- Concernant les consignes saisies, des traitements très simples permettant de limiter les conséquences d'une erreur peuvent être mis en œuvre. Par exemple, l'automate peut imposer une variation maximale de la consigne de débit barrage, et limiter ainsi à une valeur prédéfinie la variation du débit relâché à l'aval. Cette stratégie peut également être appliquée à la consigne de niveau si l'automate effectue la régulation du plan d'eau.
- Les mesures jugées critiques doivent être redondées (mesure de niveau amont par exemple) et intercomparées.
- Le comportement en cas de retour de validité de la mesure doit également être prévu.

6.3 Les contrôles internes et l'autosurveillance

Un système auto-surveillé, capable de détecter un dysfonctionnement interne et d'alerter le cas échéant est beaucoup plus sûr qu'un système non-surveillé. L'automate doit donc disposer de fonctions de surveillance interne, portant sur ses composants matériels et également sur ses traitements. Pour ces derniers, des contrôles interne permettent de s'assurer que l'on reste dans le fonctionnement prévu et de basculer dans un mode de repli et d'alerter l'exploitant si ce n'est plus le cas.

Par exemple, si l'automate élabore une consigne de débit d'une vanne, il est important de vérifier que le débit réel de la vanne reste cohérent avec la consigne, afin de détecter une anomalie qui n'aurait pas été vue par les protections de 1er rang.

6.4 Le Maintien en Condition Opérationnelle (MCO)

L'automate peut faire l'objet de mise à jour tout au long de la vie du système, pour des raisons diverses ; modification des consignes l'exploitation, évolution des caractéristiques d'une vanne, remplacement d'un capteur, correctifs, etc. Les opérations de modification de l'automate sont par nature risquées et doivent être strictement encadrées par un processus formalisé couvrant les aspects suivants :

- Traçabilité des modifications du logiciel et des paramètres
- Mise à jour de la documentation technique
- Réalisation de tests en plateforme. Il est indispensable de prévoir un environnement de test plate-forme permettant une qualification adéquate de l'automate. A cet effet, un simulateur de la partie opérative est nécessaire.
- Prévoir des tests de non-régression permettant de garantir que les fonctions non impactées par les évolutions le sont effectivement.
- Préparation des essais sur site sur la base d'une analyse de risques.
- Traçabilité complète des tests effectués en plate-forme et sur site.

6.5 Utilisation d'un référentiel technique et d'amélioration continue

Pour un exploitant de plusieurs barrages, il est possible de définir une stratégie basée sur l'utilisation d'un référentiel commun à l'ensemble de automates en exploitation. Cette stratégie permet :

- Une cohérence fonctionnelle entre les différents automates en exploitation sur le parc.
- L'utilisation de modules logiciels standards « durcis » qui font l'objet d'une qualification renforcée.
- Ces modules étant utilisés sur plusieurs automates, de bénéficier d'un retour d'expérience (REX) au périmètre d'un parc ce qui permet une amélioration continue du référentiel technique. Plus le parc est important, plus ce REX est favorisé et meilleur sera le référentiel.

7. CONCLUSION

L'approche utilisée par CIH pour coter les défaillances des automates permet d'avoir une cotation plus fine et reflète mieux les améliorations apportées progressivement au référentiel technique d'EDF Hydro. Les automates développés récemment, conformes aux standards actuels, devraient bénéficier d'une meilleure cotation ce qui est cohérent avec l'attention portée au renforcement de la sûreté dans les derniers référentiels.

La clarification des modes de défaillances (non-fonctionnement / dysfonctionnement) ainsi que des causes de ces modes de défaillances permettent d'identifier les contrôles et les points clés à mettre en œuvre et à respecter en maintenance. En ce sens, le travail sur la méthodologie de cotation d'un automate va dans le sens de la sûreté.

Pour les automates plus anciens, l'approche par indice de confiance permet de faire un état des lieux précis des automates et d'avoir ainsi une vision claire de leurs faiblesses potentielles. En complément d'autres approches, elle contribue à améliorer la vision patrimoniale du parc d'automates en exploitation. Ces résultats peuvent conduire à prioriser des opérations de rénovations du contrôle-commande du barrage s'il s'avère que les automates induisent des risques trop importants.

RÉFÉRENCES ET CITATIONS

[1] INERIS - Probabilité dans les études de sécurité et études de dangers - OMEGA 24 N° DRA-18-171229-00933A

[2] INERIS - Agrégation semi-quantitative des probabilités dans les études de dangers des installations classées - OMEGA 25 N° DRA-18-171229-00918A