Introduction

La détection d'anomalies en l'absence d'historiques de défauts (en mode aveugle) dans les données industrielles nécessite la caractérisation du ***domaine de normalité***. Deux classes d'approches se portent candidates à la résolution de ce problème encore ouvert : **les approches *basées sur les données*** et les approches par ***jumeaux numériques***. Les deux classes viennent *au pluriel* car pour chacune d'elles, beaucoup de variantes sont possibles. En réalité, un continuum de variantes existe allant de l'approche purement « *données* » à la modélisation physique la plus fine, les variantes intermédiaires incorporent ici et là des petites boîtes noires identifiées par des approches basées sur les données donnant ce qui est désigné par modèle en boîte grise. Pour souci de clarté, nous regardons uniquement les deux extrêmes pour en définir les contours, les promesses, les avantages mais aussi *la poussière que l'on cache souvent sous le tapis*. Pour ce qui est du périmètre de la discussion, nous nous limitons à la problématique de **détection d'anomalies, en mode aveugle**, à partir des séries temporelles issues d'équipements industriels.

Commençons par présenter brièvement les deux approches avant d'entamer la discussion.

Jumeaux numériques

Dans le sens le plus communément utilisé, un jumeau numérique est un modèle informatique/mathématique permettant de **simuler l'équipement** en réponse à **toute** excitation exogène possible. Ce modèle traduit les connaissances scientifiques sur les lois régissant le comportement de l'équipement (par exemple : équations de Lagrange, lois de la thermodynamique, loi de conservation, loi de transfert et de transport pour ne citer que quelques exemples). L'ensemble des grandeurs intervenant dans le modèle se divisent en plusieurs catégories :

- **Les variables d'état** (x) : les grandeurs décrivant l'état du système
- **Les données exogènes** (w) : les grandeurs influant le comportement du système qui ne se déduisent pas des précédentes et qui en sont indépendantes (consignes, perturbations, mode de fonctionnement)
- **Les paramètres** (p) : ce sont les données constantes ou lentement variables souvent inconnues (coefficients de frottement, état de surface, inertie mécanique ou thermique, coefficients aérodynamiques, etc.). Il est commode pour la discussion de penser **les anomalies comme des changements dans certains paramètres de l'équipement.**
- **Les mesures** (y) **:** Ce sont les grandeurs que l'on peut mesurer. Ce sont en général des expressions mêlant les composantes du vecteur d'état et des paramètres du système.

Ainsi, un jumeau numérique inclut des expressions de la forme :

$$\left(\text{Équation d'évolution}\right)\ \ x^{+} = f(x, w, p) \qquad \left(\text{Équation de mesure}\right)\ \ y = h(x, p) \qquad (1)$$

La première prédit la valeur future de l'état du système en fonction de son état actuel (x), des données exogènes (w) et des paramètres supposés du modèle (p). La seconde prédit les mesures obtenues par les capteurs. Du coup, une série temporelle de mesures Y contenant le passé des sorties capteurs sur un fenêtre prend la forme suivante :

$$\left(\text{Prédiction d'une série temporelle de mesures}\right) \qquad Y = F\left(x_0, w(.),\ p\right) \qquad (2)$$

Puisque les mesures collectées dépendent des valeurs successives de l'état qui dépendent de l'état initial (en début de la fenêtre d'observation) et des profils des données exogènes ainsi que des paramètres réels du système.

> La promesse des jumeaux numériques dans le contexte du problème de détection d'anomalies en mode aveugle est de pouvoir détecter une anomalie (changement de paramètre p) à partir de la détection de l'écart entre les séries temporelles mesurées et les séries temporelles prédites

Approches sans modèle basées sur les données

Dans ces approches, les comportements des séries temporelles sont analysés sans chercher a priori à en connaître les causes. L'analyse consiste à mettre en évidence un ensemble de relations (invariantes) satisfaites sur les données d'entraînement (supposées saines) et robustes vis-à-vis du critère de la validation croisée. Contrairement à l'approche précédente, ici, la causalité est moins présente et la normalité est définie par l'appartenance d'un ensemble d'indicateurs à des domaines pris comme **les plus petits possibles** permettant néanmoins de concilier les données saines d'apprentissage avec un taux de faux-positif prescrit à l'avance.

Il va de soi que le nombre de ces indicateurs et les relations qui les justifient ne peuvent pas être connus a priori si l'on exclut une analyse physique de type modèle de connaissance. Ils convient alors d'en générer un nombre important selon diverses hypothèses afin de tenter de cerner au mieux la situation en mode aveugle.

> L'intuition derrière les méthodes basées sur les données est que si les **domaines de normalité sont minimaux** et conduisent à un faible taux de faux positifs même sur des centaines de milliers d'instances saines non vues pendant l'apprentissage alors une sortie de la normalité déclarée sur de nouvelles mesures doit être prise au sérieux. D'autre part, si malgré l'utilisation d'un **nombre important de tels domaines** aucun des indicateurs associés ne sort de la normalité, alors la probabilité d'une anomalie doit être considérée comme faible.

Discussion

Il est souvent considéré qu'un jumeau numérique serait le meilleur choix s'il n'était pas trop coûteux à produire car nécessitant un savoir-faire pointu associé à chaque domaine spécifique. Il s'ensuit que si l'enjeu est suffisamment important pour justifier d'y mettre les moyens, alors le choix est clair. Les quelques éléments de réflexion qui suivent mettent en doute la véracité de cette affirmation.

Tout d'abord, conceptuellement, tout modèle doit être calibré en fonction de l'usage que l'on veut en faire. Il paraît clair que **détecter une anomalie ou simuler un procédé sont deux usages très différents**. Le jumeau numérique n'est a priori pas nécessairement adapté.

D'autre part, en règle générale, les équations régissant les systèmes dynamiques comme les équipements industriels sont bien connues uniquement sous certaines hypothèses (gaz parfait, liaisons sans frottement sec, roulement sans glissement, équilibre thermodynamique, milieux homogènes, mélanges parfaits, liaisons parfaites, etc.). Or ces conditions sont violées même dans le cas considéré comme sain et du coup, même en l'absence d'anomalie, ces équations ne sont qu'approximatives. La comparaison de leur prédiction avec les mesures réelles risque de générer des faux positifs, parfois fréquents à cause d'écarts importants mais brefs issus de phénomènes non modélisés car difficiles à appréhender.

Même si la structure des équations était connue, les valeurs numériques des paramètres doivent être identifiées à partir des mesures. Ceci passe par un processus d'optimisation généralement non convexe et à l'issue incertaine car cela dépend de la qualité des données permettant d'acquérir une information complète évitant qu'une combinaison erronée de paramètres ne viennent *concilier les mesures*.

A supposer que les paramètres sont correctement identifiés, selon le principe de l'utilisation des Jumeaux numériques pour la détection d'anomalies résumé dans l'encadré plus haut, la comparaison entre le modèle et la réalité doit se faire sur des fenêtres d'observation à états initiaux (x0) identiques de telle sorte que seuls les vecteurs de paramètres diffèrent entre la réalité et le modèle nominal simulé. Or dans presque la majorité des cas, **toutes les composantes du vecteur d'état ne sont pas accessibles à la mesure**, du coup, pour effectuer la comparaison ci-dessus, un estimateur d'état est nécessaire afin de soumettre les modèles à la comparaison. Or **le principe même de l'estimateur d'état est précisément de trouver un état tel que le modèle simulé produise les mêmes sorties des capteurs que celles mesurées** ! Cet algorithme fera donc tout ce qu'il est en son pouvoir pour **compenser le changement paramétrique (l'anomalie) par une mauvaise estimation de l'état de telle sorte que tout apparaît normal du point de vue des mesures**. Cette mauvaise estimation de l'état ne sera pas détectable car l'état lui-même n'est pas mesuré ! Ce risque n'existe pas dans le cas de modèles dits à observabilité étendue (observabilité des états et des paramètres par les mesures) ce qui est non seulement très rare mais génériquement impossible à vérifier pour des équipements industriels complexes réels.

Pour finir, on pourrait croire que le jumeau numérique offrirait une meilleure explicabilité des anomalies. Ceci n'est vrai que sous deux conditions :

1. Chaque anomalie potentielle est associée à un ou plusieurs paramètres du modèle
2. Le modèle résultant est à observabilité étendue au sens expliqué plus haut.

Ces conditions sont difficiles à satisfaire car la compréhension des phénomènes anormaux est beaucoup moins accomplie que les phénomènes régis par la situation nominale et que plus on entre finement dans la modélisation de ces situations critiques, moins la satisfaction de la deuxième condition devient probable.

Contrairement aux jumeaux numériques où le concept d'état est indispensable avec son cortège de problèmes d'ambiguïté et de nécessité de recalage, l'approche basée sur les données ne traite que les relations internes dans l'historique des mesures d'un capteur ou les relations inter-capteurs à la recherche d'invariants spécifiques et leur domaine ayant les propriétés énoncées plus haut. La possibilité, pour une approche de type données, de travailler sur des sous-groupes de capteurs voire sur un seul capteur si l'intuition le suggère est totalement incompatible avec **l'approche holistique des jumeaux numériques** où par définition, tout ce qui vit au sein de l'équipement doit être inclus dans un seul et même bloc : le simulateur ! Il s'ensuit que l'approche basée sur les données est plus souple et modulaire ce qui vient avec des avantages certains sans pénaliser la productivité puisque le coût de production des modules de solutions associés est négligeable comparé à celui des jumeaux numériques.

De plus, comme c'est le cas chez Amiral-Technologies, la génération même de ces invariants puise ses intuitions dans les structures génériques de modèle de connaissance sans pour autant en supporter les inconvénients. Si l'explicabilité serait moins précise qu'un idéal irréalisable (comme montré plus haut), un certain niveau de localisation des sources d'anomalie (en un sous-groupe limité de capteurs participant dans la définition de l'invariant *rebelle*) reste accessible et facilement calculable.

Cette réflexion ne clôt certainement pas ce débat technique et passionnant. Permettrait-il au moins de rendre moins sûres des affirmations souvent considérées comme allant de soi ?

Sébastien Le Gall, CTO chez Amiral Technologies