L'INTEROPERABILITE DANS LES POSTES PCCN

Olivier JARAY (1) Jean-Pierre THOMESSE (1),
Jean-Philippe TAVELLA (2)
(1) LORIA-INPL, 2 av. de la Forêt de Haye, 54516 Vandoeuvre lès Nancy, France
Tél : 33-3-83-59-55-76, Fax : 33-3-44-07-63
mél : {ojaray,thomesse}@loria.fr
(2) EDF-DER, 1 av. du Général de Gaulle, 92141 Clamart
Tél : 33-1-47-65-35-61, Fax : 33-1-47-65-46-88
mél : { jean-philippe.tavella}@der.edfgdf.fr

RESUME

Le développement et les performances de la technologie des réseaux et des ordinateurs ont conduit à la définition d'applications distribuées plutôt que centralisées.

Un système donné peut ainsi être composé de sous-systèmes (ou lots) provenant de constructeurs différents. Si cette solution est techniquement et économiquement intéressante, elle ne peut être utilisée que si l'intéropérabilité entre les différents lots est garantie et vérifiée.

Cet article présente ces problèmes et propose une solution basée sur la modélisation formelle.

MOTS-CLES

Interopérabilité, méthodes formelles, tests de conformité, génération automatique.

1. INTRODUCTION

Systèmes ouverts, hétérogénéité, interopérabilité, interfonctionnement sont les mots clés des systèmes distribués. L'évolution des systèmes ouverts, accélérée par les nouvelles possibilités offertes par les réseaux de communication, a conduit les fournisseurs d'électricité à concevoir l'architecture du poste de manière ouverte et sur une base numérique. Le projet PCCN de EDF [5], [6] en est un exemple type. PCCN signifie "Protection et Contrôle Commande Numérique " et correspond à une architecture divisée en cinq catégories de lots définies selon des critères économiques et techniques.

Le but du projet PCCN est de concevoir un nouveau palier dans le contrôle commande des postes HTB/HTA. Le projet matérialise le besoin de remplacement des postes EDF par du matériel numérique, pour améliorer leur fiabilité, réduire leur coût de maintenance et compenser la vétusté des équipements.

L'objectif principal des systèmes ouverts est la réduction des coûts induite par la mise en concurrence des constructeurs [9]. Toutefois, cette option présente des difficultés que l'on ne rencontre pas lors de l'achat de système propriétaire clé en main.

Une politique de choix de systèmes ouverts nécessite entres autres des efforts de spécification avant la construction du système puis des tests de conformité et de qualification des sous-systèmes puis enfin d'intégration. Avec un système ouvert, c'est à l'utilisateur de vérifier l'interopérabilité des lots d'origines différentes. Le projet PCCN en est en fait à cette étape. Les cinq lots ont été confiés à différents fournisseurs, ayant la responsabilité de deux ou trois lots chacun, et il appartient à EDF, en tant que maître d'ouvrage, de réaliser leur intégration et de traquer les cas de non interopérabilité. EDF doit alors être capable de déterminer quel sous-système est en cause.

Cet article présente ces problèmes et leurs solutions qui appartiennent aussi au domaine des sous-systèmes hétérogènes. Afin d'expliciter la solution proposée, la deuxième partie décrit l'architecture du système PCCN vis à vis de la communication en montrant les problèmes à résoudre. Dans une sous-partie, le nouveau protocole "M-PCCN " sera brièvement présenté.

La troisième partie présente l'approche définie par EDF et les tests qui doivent être réalisés. La dernière partie développe la méthode, basée sur la description formelle, utilisée pour la réalisation des tests décrits dans la troisième partie.

Nous conclurons sur les avantages et les inconvénients d'une telle méthode.

2. CONTEXTE

2.1. Architecture du système

Le diagramme suivant présente l'architecture du système de contrôle/commande des postes HTB/HTA représentés sous la forme de lots connectés au réseau de communication. Chaque lot représente un seul ensemble ou plusieurs équipements connectés grâce à un réseau interne spécifique au lot (et au fabricant).

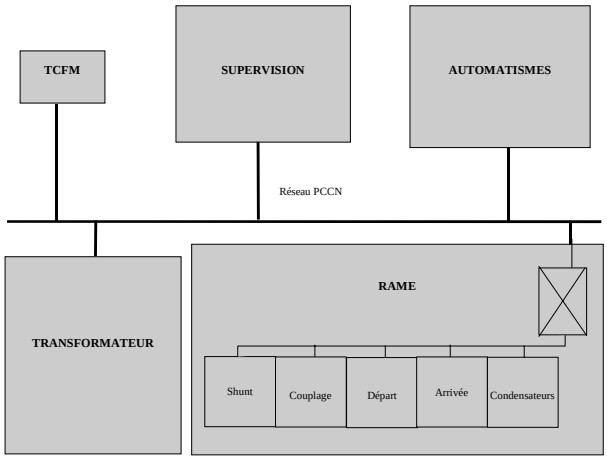

Figure 1 : Architecture du système

Les fonctionnalités des différents lots sont brièvement décrites ci dessous:

- Supervision : consignation de tous les événements du système, contrôle local (y compris la gestion de réseau) et contrôle distant (interface avec un réseau longue distance) ;
- Automatismes : fonctions d'automatismes distribués comme la permutation des transformateurs ou la régulation de tension ;
- Rame : détection des défauts et protection du jeu de barres ;
- Transformateur : protections internes et externes des transformateurs, protections des auxiliaires.

2.2. Architecture d'un lot

Le réseau de communication est un réseau Ethernet sur fibre optique à 10 Mb/s. Les protocoles de communication choisis pour réaliser les besoins de contrôle numérique des lots sont ceux décrits ci-dessous :

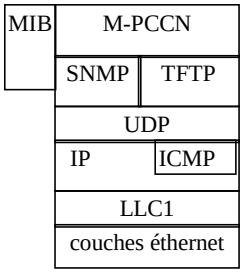

Figure 2 : Pile de protocoles

Tous les lots du réseau doivent posséder cette pile de protocoles. La couche application contient tous les processus de niveau application communicant grâce à la couche M-PCCN basée sur les standards SNMP et TFTP.

Tous les objets sont définis et structurés en conformité avec les règles de la MIB (Management Information Base) SNMP.

Ce système de communication doit transmettre des données MIB pour lire, écrire ou effectuer des actions. Ces données sont des états (appelées TS doubles), des événements (appelés TS fugitives), des commandes (appelées TC), des mesures (TM) ou des fichiers.

L'échange de données en temps réel peut être divisé en deux catégories :

- des données évolutives dont la valeur reflète l'état d'un événement du procédé ou du système de contrôle commande ou un événement durable. Dans le PCCN, on gère des états binaires (valeur 0 ou 1 qui reflète un état fermé ou ouvert, en service ou hors service, …) et des états 1 parmi n;
- des données événementielles qui ne présentent d'intérêt que ponctuellement. Ce type de données peut être un événement fugitif (événement ayant un intérêt ponctuel), une commande (demande d'action pour provoquer le changement d'état d'un élément du processus ou du système de contrôle commande), une requête (commande sans acquittement), une consigne ou un fichier.

Chaque entité M-PCCN joue le rôle d'agent SNMP ou de gestionnaire suivant sa position de producteur ou consommateur, client ou serveur.

Pour échanger ces objets, les services suivants ont été définis :

- CDE : pour agir sur un organe ou une fonction distante
- EF : pour transmettre un événement fugitif
- ETAT : pour signaler un changement d'état
- CONS : pour transmettre une consigne
- LCONS : pour lire une consigne distante
- MES : pour mettre à jour une mesure locale
- LMES : pour lire une mesure distante
- DOWNLOAD : pour transférer un fichier
- UPLOAD : pour rapatrier un fichier
- REQ : pour transmettre une requête
- CNX/DNX : pour établir la connexion ou la déconnexion d'un lot sur le réseau et pour contrôler en permanence les lots connectés.

Ces services ont été définis dans la couche M-PCCN pour satisfaire aux missions définies plus haut.

3. L'APPROCHE EDF

Pour le projet PCCN, EDF a défini trois étapes menant à une validation complète du système. Ces étapes sont présentées et illustrées dans cette partie.

3.1. Qualification

Etant donné qu'un lot peut être vu comme un ensemble d'équipements, chacun d'eux est d'abord testé séparément. La pile de protocoles (cf. partie 2) est un des composants et sera considéré à part dans cette section.

Nous faisons l'hypothèse ici que l'implémentation des protocoles sous-jacents à M-PCCN est entièrement conforme aux standards.

Dans ce contexte, la phase de qualification inclut les tests de conformité et de robustesse de l'implémentation du protocole M-PCCN.

Le test de conformité est divisé en deux étapes. La première est la validation de la MIB. Elle consiste à vérifier que tous les objets sont correctement structurés et qu'il est possible de les lire ou de les modifier. La seconde étape doit permettre de valider les services un par un. On doit s'assurer que le lot réagit comme cela a été défini dans les spécifications.

Le but du test de robustesse est de vérifier le fonctionnement dans des situations critiques. Dans ce cas, les suites de tests sont directement issues de la connaissance du système et de l'application. Nous réalisons une rafale de services SNMP pour être sûr que le système réagit toujours correctement. Par exemple, on envoie à un lot une rafale de 10 SET ou GET et on vérifie qu'ils sont bien tous pris en compte.

3.2. Recette

La recette a pour objectif d'être sûr qu'un lot est capable de communiquer et d'interopérer avec une plate-forme de test qui est en fait un modèle des autres lots et du processus électrotechnique.

La phase de recette doit vérifier que le lot est capable d'échanger correctement les bonnes PDU avec le testeur. Il est composé de deux étapes :

- le choix des suites de test est fait et l'ITU (Implementation Under Test) est positionné sur le bon état ;
- un processus applicatif particulier qui peut être considéré comme un automate est démarré et les échanges sont enregistrés.

Pour chaque test le résultat peut être " succès " ou " échec ". Dans les normes sur les méthodes de test de conformité, le résultat peut être " succès ", " échec " ou " non décidable ". Dans l'approche de la recette M-PCCN sur les tests, un résultat non décidable est considéré comme un échec.

3.3. Intégration

Le but de la phase d'intégration est de vérifier pour un lot donné qu'il est capable d'interfonctionner avec un ou plusieurs autres lots réels. A la fin d'une phase de recette réussie, un lot est considéré comme " accepté " dans l'environnement de simulation du testeur. Lors de la phase d'intégration, les lots simulés sont remplacés par des lots réels qui sont aussi passés avec succès par l'étape de recette. L'intégration est réalisée de façon progressive, c'est à dire que l'on remplace graduellement les simulateurs par les lots réels. Néanmoins, à part pour le dernier essai (comprenant exclusivement des lots réels), la plate-forme de test est toujours utilisée pour la simulation.

3.4.La plate-forme de test

La plate-forme est la même pour la recette et l'intégration. Elle est composée de :

- un ensemble de simulateur de lots;
- un simulateur du procédé électrotechnique;
- un point d'observation;
- un gestionnaire de test.

Le schéma suivant montre l'architecture globale de la plate-forme de test. Une seconde architecture simplifiée (sans simulation du procédé électrotechnique et sans simulateur de lots) est utilisée pour la qualification de la pile de communication.

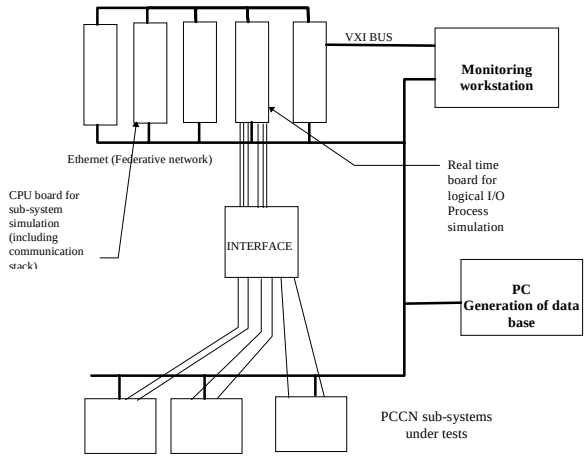

Figure 3 : Plate-forme de test

L'IUT est un lot réel avec sa pile de communication et ses processus d'application. Comme un lot réel, il est connecté au testeur à travers un réseau Ethernet réel et au simulateur du procédé électrotechnique grâce à ses propres entrées et sorties.

Le procédé électrotechnique est modélisé par un automate avec un ensemble d'entrées/sorties numériques et analogiques réelles.

Un simulateur de lots est une boite noire échangeant des PDU avec son environnement comme un lot réel. Mais en fait, il peut communiquer avec le testeur directement à travers un système de communication externe utilisé pour les transferts de fichier et la planification des tests.

Le point d'observation analyse et enregistre toutes les trames échangées entre l'IUT et les simulateurs.

3.5. PICS and PIXIT

Pour faciliter l'implantation des suites de test, nous avons réalisé deux documents qui ont été distribués aux constructeurs. Le premier, appelé PICS (Protocol Implementation Conformance Statement), contient la liste des services implantés par le constructeur et tous les paramètres et temporisateurs définis dans les spécifications. Pour ces différents objets, on précise leur objet, la plage des valeurs autorisées, l'unité et le pas. Le deuxième document, appelé PIXIT (Protocol Implementation eXtra

Information for Testing) précise pour chacun des services, comment les déclencher ou les observer.

3.6. Conclusion

Nous avons présenté l'approche EDF concernant la vérification des lots et du système complet.

Les tests de qualifications englobent les tests de conformités [7]. Cependant ils sont plus complets depuis que les tests de robustesse ont été ajoutés.

Les tests de recette font partie de la famille des tests d'interopérabilité et d'interfonctionnement [1], [8]. Ils sont gérés comme pour la vérification de conformité puisqu'un seul lot est concerné à la fois. Les tests incluent réellement les processus du niveau application du lot. En ce sens, ils vérifient pour chaque lot une partie de l'interopérabilité sans distinction entre les aspects dépendants ou non de l'application [10].

Les tests de recette incluent aussi un test de robustesse.

Les tests d'intégration sont réellement des tests d'interfonctionnement.

Les suites de tests sont les mêmes dans les deux cas. Leur génération à l'aide des méthodes formelles fait l'objet de la partie suivante.

4. Les principes de la méthode formelle

4.1. Spécification et description

Les spécifications de tout le système PCCN (appelées STB à EDF) sont décrites en français. L'utilisation d'une méthode formelle diminue le risque de mauvaise compréhension de la part des constructeurs puisque les ambiguïtés inhérentes au langage naturel sont supprimées.

Nous avons tout d'abord modélisé chaque fonction grâce à une représentation états/transitions et actions sous forme de tableau. Le schéma suivant présente un exemple très réduit de cette représentation :

Etat initial	Evénement	Action	Etat final
CNX	CDE.ind	SET_req	Wait
Wait	Get_Response.ind	CDE_cnf	CNX

Figure 4 : Représentation d'automate formel

Ces spécifications formelles ne sont pas contractuelles mais sont données aux constructeurs pour qu'il puisse rapidement avoir une vue globale du système (surtout pour les lots dont le développement ne leur incombe pas).

Ensuite, pour valider l'aspect dynamique du système, nous avons choisi le langage LDS (Langage de Description et de Spécification) [2], [4].

LDS est un langage permettant la définition de systèmes états/transitions communicants à travers des primitives de services d'envoi et de réception incluant la gestion des délais. Ce n'est pas le langage le plus formel mais il a l'avantage d'être facile à lire et à comprendre.

4.2. Validation

Partant des précédentes spécifications et modèles, nous avons réalisé leur validation et vérification en utilisant la méthode suivante.

Tout d'abord nous avons utilisé l'outil de simulation du progiciel Objectgeode [11] pour simuler le modèle pas à pas. On peut ainsi vérifier le modèle sur lequel repose l'ensemble des étapes suivantes.

Pour valider les spécifications formelles, nous avons réalisé une simulation du modèle SDL et nous avons comparé les résultats aux spécifications. S'ils correspondent à ceux attendus, les spécifications formelles sont validées.

Enfin, nous avons utilisé l'outil de vérification pour détecter automatiquement les possibles deadlocks, livelocks, etc. des STB. Le schéma suivant résume cette méthode :

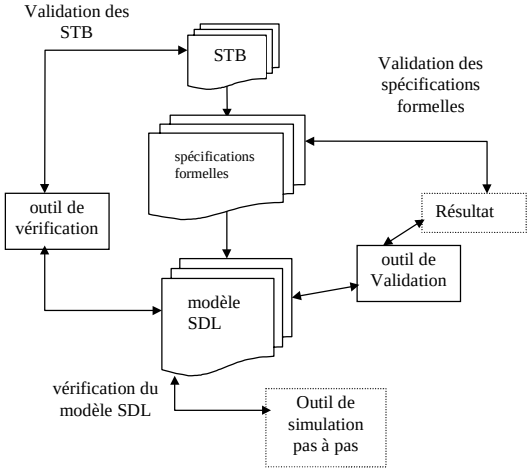

Figure 5 : Principes de validation

Après cette validation, nous pouvons utiliser le modèle LDS comme une représentation équivalente validée (mais simplifiée) des spécifications pour générer les suites de tests.

4.3. Génération de tests

Pour générer les suites de tests de l'étape de qualification, nous avons modélisé en LDS la pile de protocole sous-jacente à M-PCCN avec comme seul ambition de pouvoir acheminer un message, le perdre, le retarder ou générer des erreurs..

Puis nous avons utilisé l'outil de vérification sur le modèle LDS du système et de la pile de protocole pour générer automatiquement les scénarii. Ensuite, nous les avons représentés selon la norme MSC (Message Sequence Chart) pour modéliser les messages échangés sur le réseau entre les différentes entités. Le schéma suivant est un exemple de cette représentation:

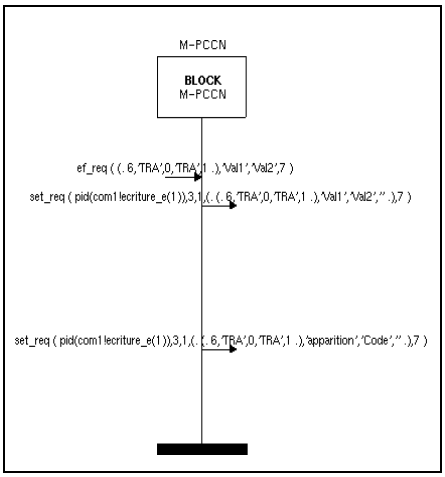

Figure 6 : représentation MSC

Les demandes de service viennent de la gauche de l'axe vertical et les messages échangés sont sur le côté droit.

Pour la phase d'intégration, une petite mais significative partie de l'application de PCCN a été modélisée en LDS. Cette étude s'est focalisée sur la permutation de transformateurs en cas de défaillance.

Comme ils sont basés sur un formalisme états/transitions, les modèles LDS décrivant le comportement de cette application mènent à une explosion du nombre d'états. Certaines simplifications ont été faites pour réduire le nombre d'états et de transitions. Mais, malgré ces simplifications, le nombre de suites de tests générées reste beaucoup trop grand pour généraliser cette méthode à l'ensemble du système PCCN.

Cependant, nous avons montré que dans l'ensemble des tests trouvés, certains étaient pertinents et non prévus par les experts électrotechniciens.

5. CONCLUSION

Dans cet article, nous avons présenté la méthode choisie par EDF pour vérifier et qualifier l'implantation des lots du contrôle commande. Cette méthodologie a été rapidement comparée avec les méthodes générales.

L'article a montré :

- l'intérêt de SDL pour la validation du protocole M-PCCN et pour la génération des tests (cf. étape de qualification et aussi la possible future norme [5]);
- le même intérêt pour la validation de la couche application malgré les limites dues au nombre d'états;
- le fait qu'une spécification formelle ait permis de résoudre plusieurs ambiguïtés présentes dans les spécifications initiales écrites en langage naturel.

Plus généralement, la méthode EDF pourrait être étendue à des réseaux et applications plus générales.

Le travail a aussi montré la nécessité d'une recherche théorique basée sur la réduction mathématique de modèles complexes en gardant la même sémantique et les mêmes propriétés que les spécifications de départ [3]. Mais, une telle étude n'était pas compatible avec les contraintes du projet en terme de délai et de budget.

Un autre axe pour la recherche pourrait être une spécification plus modulaire des spécifications de l'application en évitant l'utilisation du langage naturel.

Enfin, il serait intéressant de voir comment modéliser l'application de façon simple plutôt que de regarder comment simplifier un modèle complexe.

6. BIBLIOGRAPHIE

[1] Y. Benkhellat and J.P. Thomesse "Validation of timing properties for interoperability in distributed real time applications". Proc 13th PSTV, IFIP, Chapman and Hall, 1994, pp331-338.

[2] R. Braek "*SDL Basics* Computers Networks and ISDN Systems 28", 1996. Elsevier Science B.V.(Editeur). p1585-p1602

[3] E. Brinksma (1988). "A theory for the derivation of tests". In PSTV VIII, IFIP, Elsevier Science Publisher, pp 235-247.

[4] ITU Z100 SDL 92, "Secification and Description Language", ITU Geneva, 1994

[5] P. Godfrin, WY. Thang, G. Barssoff, "Digital protections and control-command system of HV/MV substations specification of an open architecture". DASM Europe, 1996, Vienna

[6] P. Godfrin, WY. Thang, M. Poncin, JF. Brisset, "a digital parcelled-out protection and control system of HV/MV substation". Power Delivery, 1997, Madrid.

[7] ISO IS 9646-1 to IS 9646-5. "Open Systems Interconnection OSI conformance testing methodology and framework". 1988.

[8] O. Rafiq "Sur la vérification de l'interconnexion des systèmes". In CIM'90. Bordeaux, France, 1990, pp 557-564.

[9] W.Y. Thang, JY. Boussion, B. Peruzzo, R. Hubner, "An approach for an open control system for substations", CIRED 1997, Birmingham.

[10] J.-P. Thomesse "Interoperability, an overview, SICICA", 3rd IFAC Symposium on Intelligent Components and Instruments for Control Applications. L. Foulloy Ed., 1997, Annecy, France, pp473,478.

[11] several documents on the ObjectGeode software tool :

- ObjectGeode ProjectOrganiser : Reference Manual. Version 1.3.
- ObjectGeode Method Guidelines Version 1.0.
- ObjectGeode Tutorial.
- ObjectGeode Training : Analysis and Design of Real-Time Systems.
- Verilog, 52 avenue Aristide Briand, 92220 Bagneux.