Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 81 (1990)

Heft: 5

Artikel: Installations RNIS : une nouvelle approche pour une meilleure disponibilité

Autor: Salperwyck, Luc

DOI: https://doi.org/10.5169/seals-903093

Installations RNIS – une nouvelle approche pour une meilleure disponibilité

Luc Salperwyck

Les centraux téléphoniques RNIS privés et les ordinateurs traditionnels se ressemblent comme deux gouttes d'eau. Ce fait a une incidence sur les notions de fiabilité et de continuité de service particulières que l'on peut exiger d'une installation téléphonique. Après une brève analyse des défaillances possibles, cet article présente, dans un cas concret, une nouvelle architecture d'installation de centraux téléphoniques qui a permis, pour un investissement de base pratiquement équivalent, d'améliorer sensiblement la disponibilité par rapport à une architecture classique.

Private ISDN-Telefonzentralen und herkömmliche Computer gleichen sich wie zwei Wassertropfen. Diese Tatsache ist von spezieller Bedeutung, wenn es um Zuverlässigkeit und Unterhalt von Telefonnetzen geht. Nach einer kurzen Analyse möglicher Ausfälle, stellt dieser Artikel anhand eines konkreten Falles eine neue Installationsarchitektur für Telefonzentralen vor, die im Vergleich zum klassischen Aufbau bei ähnlicher Basisinvestition eine spürbar bessere Verfügbarkeit bietet.

Adresse de l'auteur

Luc Salperwyck, Ing. Elec. dipl.
INPG/ENSERG, Elec – Engineering SA, Ingénieurs-conseils, 6, chemin de la Fruitière, 1239 Collex/Genève et 22, rue Juste-Olivier, 1260 Nyon.

La notion de sécurité rapportée aux systèmes informatiques en général, et aux PABX (Private Automatic Branch eXchange) en particulier, se scinde en deux sous-notions: d'une part la disponibilité du service (téléphonique pour les PABX), et d'autre part la protection des accès aux données (conversations, data) et des données elles-mêmes lors de leur transport. Cet article traitera plus particulièrement de la disponibilité, qui peut s'exprimer par des critères d'exigence tels que: «Cette installation doit fonctionner correctement avec une probabilité supérieure à 99,99%», ou encore «On admet un fonctionnement dégradé de l'installation durant 4 heures par an.»

On définit donc la disponibilité d'un système à partir de probabilités dans le temps. Plus précisément, elle se caractérise comme la valeur stationnaire de la probabilité pour que le système soit utilisable à un instant t donné, que ce soit de façon totale ou éventuellement partielle. A noter que la disponibilité est surtout intéressante du point de vue utilisateur; en effet, certaines astuces permettent de l'améliorer sans modifier la disponibilité intrinsèque du système.

L'amélioration de la fiabilité d'un système (fig. 1) se traduit en surcoût d'investissement pour le système de base, mais aussi en économie au niveau de l'exploitation. On observe une zone optimale dans laquelle le coût globale est minimum. Des exigences particulières de fiabilité ne permettent pas forcément de se situer dans cette zone. Il est alors opportun de définir des critères de fonctionnement «de crise» acceptables pendant un court laps de temps, qui permettent au système de se trouver dans cette zone optimale de coût-fiabilité.

Les paramètres qui influencent la disponibilité sont de nature conceptuelle (architecture du système, choix de composants fiables) ou liés à la politique d'exploitation de l'installation (surveillance du système, signalistion, localistion et réparation des pannes, reconfiguration pour fonctionnement minimum). On définit ainsi les notions de MTBF (temps moyen entre deux pannes) et de MTTR (temps moyen de réparation totale). Si l'on se place dans le cas simple d'un composant, la disponibilité peut s'exprimer par:

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

ce qui revient à considérer le fonctionnement du système comme binaire (en marche, en panne).

La disponibilité a une valeur très proche de 1, et il est souvent plus commode d'exprimer l'indisponibilité, définie comme 1-A.

Analyse des défaillances

A propos des défaillances possibles du service téléphonique d'un immeuble, on peut distinguer les causes externes au central et à l'installation (par exemple, inondation des locaux, coupure prolongée de l'alimentation électrique, explosions, sabotages, etc.)

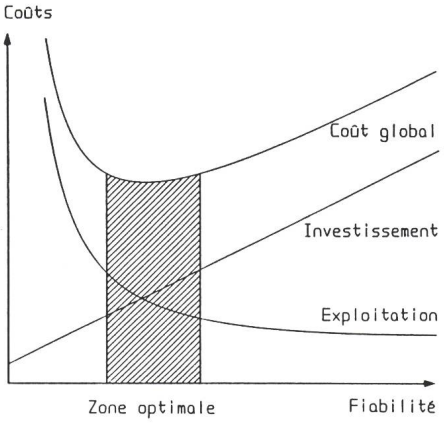


Figure 1 Fiabilité et coûts

et les causes internes, directement liées à un dysfonctionnement de tout ou partie du central. Une analyse des défaillances possibles doit donc déboucher sur une minimisation simultanée des risques dus à des causes externes ou à des causes internes.

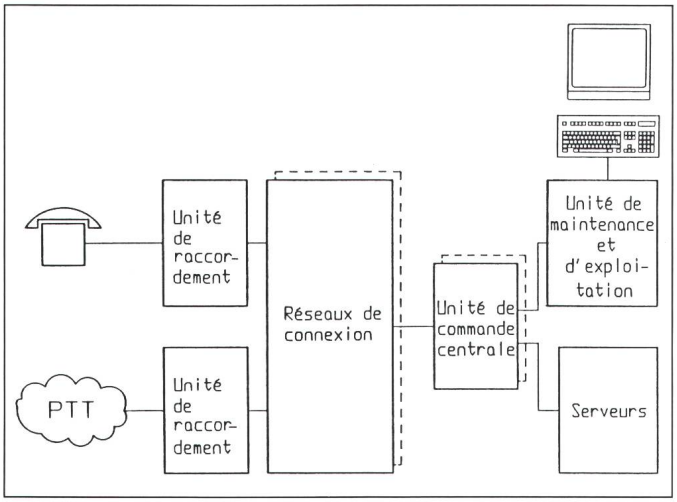


Figure 2
Architecture d'un central téléphonique

Les défaillances peuvent être scindées en deux classes, selon qu'elles touchent seulement quelques raccordements d'abonnés (nous les appellerons microdéfaillances), ou que l'installation téléphonique dans son ensemble ne fonctionne plus (macrodéfaillances). Les causes externes précédemment définies se traduisent souvent en macrodéfaillances; leur minimisation est une partie importante du travail de conception de l'installation, mais elle se situe en dehors de notre propos.

L'architecture interne des centraux, les technologies employées et la conception de l'installation téléphonique globale doivent permettre de limiter ou d'éliminer les macrodéfaillances, et de détecter les microdéfaillances d'origine interne (et éventuellement d'y remédier automatiquement). Ces notions de macro- et microdéfaillances sont assez récentes pour les centraux téléphoniques. En effet, les centraux électromécaniques d'antan étaient peu sensibles aux macrodéfaillances, car ils possédaient peu d'organes centralisés susceptibles de paralyser une grande partie de leurs raccordements.

Les centraux téléphoniques numériques actuels (nommés ECA pour Equipements de Commutation d'Abonnés) utilisent largement les techniques de traitement et de commutation numériques. Comme le montre la figure 2, ils sont schématiquement constitués d'un calculateur (unité de commande centrale), de champs de couplage temporel (réseaux de connexion), d'interfaces (unités de raccordement) et de calculateurs périphériques (maintenance et exploitation du système, serveurs). Ce type d'architecture permet une grande souplesse, notamment pour les interfaces de raccordement et les terminaux. Ainsi, les centraux compatibles RNIS (Réseau Numérique à Intégration de Service) supportent une grande variété de terminaux, depuis les postes analogiques classiques jusqu'aux stations RNIS dotées d'un interface S (2B + D à 144 kbit/s). Chaque raccordement est traité logiquement de façon semblable par la commande centrale et par les réseaux de connexion.

Les calculateurs sont d'architecture classique, basée sur des bus standards (Multibus, VME) ou autres, reliant leurs différents éléments: processeurs de traitement, mémoire de travail, processeurs d'entrée/sortie, mémoire de masse (disque dur).

Ainsi, les causes des défaillances touchant ces équipements électroniques peuvent être divisées en causes liées au matériel, au logiciel, et aux opérateurs humains.

Défaillances liées au matériel

Les défaillances du matériel électronqiue apparaissent de façon aléatoire, plus fréquemment au début et à la fin de la vie des équipements. Selon la taille et la complexité des équipements, ces défaillances de composants peuvent diminuer la disponibilité d'un système en dessous d'un seuil acceptable pour un cas donné.

La structure d'un ECA (Equipement de Commutation d'Abonnés) est de type série, c'est-à-dire constituée d'unités dont le bon fonctionnement de chacune est nécessaire au bon fonctionnement du système (fig. 3a). L'indisponibilité globale du système est alors la somme des indisponibilités de chaque unité.

La technique couramment employée pour augmenter la fiabilité de telles structures est la redondance (fig. 3b), qui peut être appliquée soit au niveau des unités ayant la moins bonne fiabilité, soit au niveau du système entier.

La redondance est caractérisée par son ordre, c'est-à-dire par le nombre de composants ou d'unités mis en parallèle. On distingue la redondance active, pour laquelle les n unités ou une partie des n unités sont constamment opérationnelles (redondance active totale ou partielle); de la redondance par commutation, pour laquelle l'unité en service n'est remplacée par une autre que lorsqu'elle présente des signes de défaillance. Le calcul de l'indisponibilité dépend lors du type de redondance; il vaut grosso modo le produit des indisponibilités des unités mises en parallèle. Il faut noter que la redondance, si elle augmente la durée entre deux pannes totales du système, augmente le nombre de réparations, du fait de la multiplication du nombre d'unités qu'elle engendre.

La redondance peut permettre de fiabiliser un maillon constitué d'unités peu fiables (fig. 3c) ou de multiplier toutes les unités une par une (fig. 3d), voire le système dans son entier (fig. 3e). Dans certains cas, elle peut même utiliser des techniques de vote majoritaire sur les sorties de chaque sous-système afin de les découpler au maximum.

L'intérêt principal de la redondance est le recouvrement automatique et immédiat des défaillances, avec des pertes d'information inexistantes ou acceptables. On peut ainsi différer l'intervention humaine pour la réparation. Cela induit le concept fondamental d'auto-diagnostic du système. Selon le cas, ce diagnostic peut être réalisé par auto-test des unités avec l'aide du logiciel (cas des petits systèmes), ou par un véritable «processeur de diagnostic» dont le seul rôle est d'émettre des stimuli de test, de recevoir les vecteurs correspondants, d'analyser le fonctionnement et de prendre les déci-

sions pour activer les unités en bon fonctionnement (cas fréquent pour les gros systèmes, par exemple mainframes). Dans tous les cas, les circuits doivent être testables, c'est-à-dire posséder deux propriétés essentielles: la *gouvernabilité* et l'*observabilité*.

La gouvernabilité est la faculté d'un circuit à permettre la propagation de signaux de tests dans ses moindres recoins (exploration des chemins de propagation), moyennant l'application de stimuli adéquats sur ses points d'entrée. L'observabilité est la faculté d'un circuit à permettre la collecte des informations de test après passage par les différents chemins de propagation, ces informations étant récupérées sur

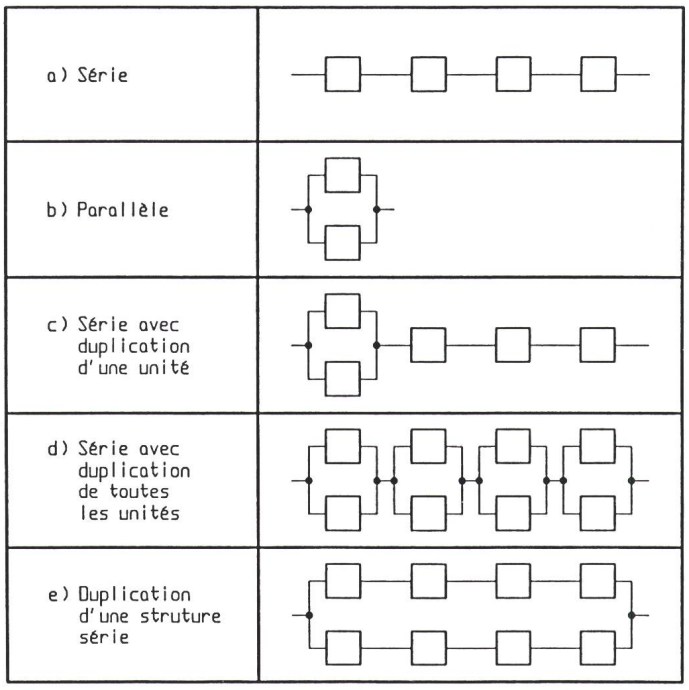


Figure 3
Structure générale d'un système

les points de sortie. La conjonction de ces deux propriétés au niveau des circuits intégrés et des macrosystèmes évite donc les zones d'ombre non testables et accroit l'efficacité de la redondance.

Ces notions de testabilité, devenues essentielles pour la conception, tant des circuits intégrés que des macrosystèmes, à cause de la complexité croissante des équipements, sont largement appliquées depuis environ une quinzaine d'années dans les architectures des gros ordinateurs mais le sont beaucoup moins sur les petits systèmes. En effet, outre les surcoûts de matériel qu'il entraîne, le diagnostic de défaillances peut exiger de puissants algorithmes de traitement, relevant parfois du domaine de l'intelligence artificielle (systèmes experts).

Les techniques de redondance sont complexes à mettre en œuvre de façon exhaustive. Même lorsqu'elles sont utilisées, il arrive fréquemment qu'un «talon d'Achille» subsiste dans le système, malgré les meilleures précautions. Par exemple, certains bus sont communs à plusieurs unités redondantes, et un collage logique des signaux de ce bus perturberait toutes les unités connectées. En ce qui concerne les ECA, la redondance n'est pas systématiquement utilisée; seuls les modèles les plus gros (en nombre de raccordements supportés) sont conçus en utilisant cette technique pour les champs de couplage et la commande centrale.

Défaillances liées au logiciel

Les défaillances inhérentes au logiciel existent bel et bien et sont «justifiées» par l'aspect humain (donc sujet à l'erreur) de la conception et surtout de la mise à jour des logiciels.

Les meilleures batteries de test et les fonctionnements probatoires ne peuvent pas garantir qu'un logiciel est exempt de bogues, car l'ensemble exhaustif des situations auxquelles il sera confronté est quasi impossible à simuler. Le facteur temps permet d'illustrer cet argument: les logiciels qui testent la date courante doivent être contrôlés spécifiquement, car les calendriers (mêmes adaptés) présentent des effets de bord parfois surprenants.

De plus, la complexité des logiciels accroît également les risques d'erreur en cas de mise à jour. Ainsi, la modification d'un paramètre peut se répercuter, de façon cachée, sur beaucoup d'autres.

On notera enfin qu'une défaillance due au logiciel se manifeste avec un caractère aléatoire, même si elle existe depuis la mise en œuvre du système.

Défaillances liées aux opérateurs humains

Parmi les autres défaillances possibles, on peut observer celles résultant d'un comportement normal du système face à un événement illogique de son environnement, comme les erreurs d'intervention humaine, fréquentes et quasi inévitables. Elles sont souvent dues à la négligence (alarmes ignorées, sauvegardes inadaptées), à l'incompétence, voire à la malveillance. Les pannes générales de système dues à la volonté déplacée d'un opérateur de maitriser la machine en s'y substituant sont assez courantes.

En résumé, la disponibilité des ECA ne saurait être garantie à 100% pour le système dans son entier, même si celui-ci possède des unités redondantes. Ce point altère quelque peu les chiffres annoncés par les fabricants d'ECA. En effet, les valeurs annoncées, typiquement le MTBF par raccordement pour une période donnée, n'ont plus de sens depuis la disparition des derniers centraux électro-mécaniques. Il convient donc de bien définir correctement les critères de disponibilité d'une installation téléphonique en ne considérant pas les centraux comme des systèmes invulnérables.

Application

L'installation téléphonique RNIS d'une grande banque privée de la place de Genève, la Discount Bank and Trust Company (DBTC), va servir d'illustration aux concepts exposés précédemment. Cette installation doit assurer la transmission des conversations téléphoniques, de données et d'images au sein de la banque et vers l'extérieur.

La DBTC est installée dans deux immeubles situés en zone urbaine et distants d'environ 900 mètres. Ces

deux immeubles accueillent des services différents et complémentaires de la banque; par conséquent, une éventuelle rupture du service téléphonique dans l'un d'eux perturberait le fonctionnement de la banque dans son ensemble. Le critère de disponibilité retenu peut donc s'énoncer ainsi: «En cas de défaillance d'un macro-élément, au moins 50% des raccordements téléphoniques de chaque immeuble doivent être opérationnels.»

Une liaison constituée d'un faisceau de trente fibres optiques multimodes (gradient d'indice) relie les deux immeubles en point à point. Cette liaison, prévue et commandée dès le stade d'avant-projet de l'installation, doit supporter l'ensemble des transmissions inter-immeubles. Par ailleurs, chaque immeuble est relié indépendamment à un seul et unique central public PTT et les faisceaux de câbles empruntent des chemins différents.

Face à un problème de ce type, la démarche de l'ingénieur consiste à concevoir une installation possédant les meilleures caractéristiques de fiabilité, de sécurité et de continuité du service pour un coût minimum.

Par définition, on exprime le caractère plus ou moins indispensable du bon-fonctionnement d'un équipement donné pour assurer le bon-fonctionnement de l'installation dans son ensemble, selon les critères de disponibilité retenus, par une expression du type (*N*-i), où i représente le nombre d'équipements annexes pouvant suppléer l'équipement donné, s'il tombe en panne. Ainsi, une installation téléphonique à fiabilité (*N*), dont un macro-élément tombe en panne, n'assurerait plus aucun service téléphonique; avec une fiabilité (*N*-1), 50% des raccordements seraient encore opérationnels dans le cas de cette panne; de même, avec une fiabilité (*N*-2), deux possibilités sont offertes pour le maintien de 50% des raccordements opérationnels. Dans notre cas, une installation à fiabilité (*N*-1) coûtant 1,1 ou 1,2 fois le prix d'une installation à fiabilité (*N*) serait une excellente alternative; si la sécurité (*N*-1) est atteinte par un doublement des coûts par rapport à la sécurité (*N*), l'alternative n'apporte aucun intérêt, ni économique pour le Maître de l'Ouvrage, ni même intellectuel pour l'ingénieur.

Cinq variantes de configuration de centraux téléphoniques ont été proposées au Maître de l'Ouvrage, offrant des degrés de fiabilité plus ou moins élevés. Ces variantes sont schématisées en figure 4.

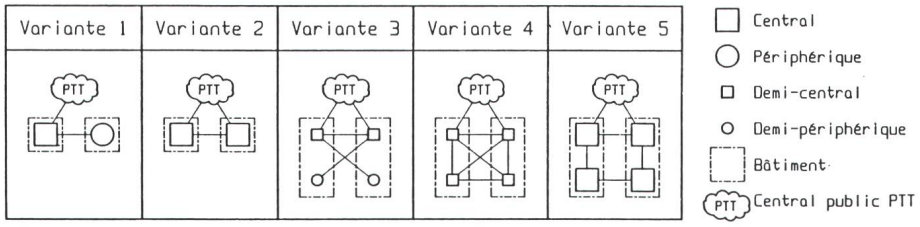


Figure 4 Variantes étudiées

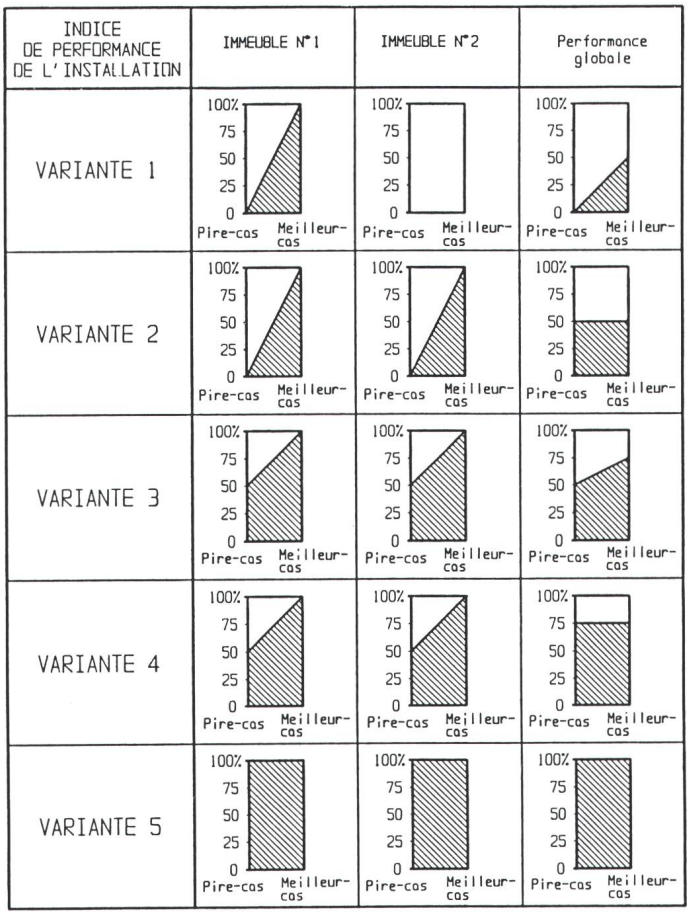
La première de ces variantes utilise un central dans le bâtiment principal, dont une partie des réseaux de connexion et interfaces de raccordement a été déportée dans l'autre bâtiment. La commutation des internes se fait au niveau local, mais la commande est centralisée dans le bâtiment principal.

Dans la suite, nous appellerons «périphérique» (ou Unité Périphérique Distante, UPD) une telle partie déportée de central, le terme «central» étant réservé à l'équipement doté de la commande centrale. De plus, les centraux et les périphériques seront considérés comme des macro-éléments.

La seconde variante utilise deux centraux distincts, un par immeuble, reliés par fibre optique en réseau. Le terme «réseau» a ici une signification analogue à celle utilisée en informatique; il désigne un ensemble d'entités indépendantes, reliées entre elles pour un partage des données et des ressources communes. Le but est que chaque utilisateur dispose d'une installation virtuellement unique (réseau transparent).

La troisième variante reprend les principes combinés des variantes 1 et

Figure 5 Analyse des macrodéfaillances par variante



2. Chaque central est relié à son propre périphérique disposé dans l'autre immeuble; les deux centraux sont reliés en réseau. Dans chaque immeuble, les raccordements dépendent, pour moitié du central de cet immeuble, et pour moitié du périphérique du central de l'autre immeuble; pour cette raison, nous appellerons de tels macro-éléments «demi-central» et «demi-périphérique».

La quatrième variante est une extension de la variante 3. Chaque bâtiment dispose de deux demi-centraux supportant chacun la moitié des raccordements du bâtiment. Les quatre demi-centraux sont reliés en réseau maillé.

La cinquième variante propose une redondance complète. Chaque bâtiment dispose de deux centraux complets, dont l'un sert de couverture passive en cas de défaillance du central actif.

Une analyse de fiabilité en cas de macrodéfaillance a été faite pour ces cinq variantes. Elle consiste à calculer, par immeuble, le pourcentage de raccordements qui seront disponibles dans le cas d'une panne d'un macro-élément. Les résultats en sont donnés à la figure 5. Ces graphiques montrent que les variantes 1 et 2 sont inacceptables en regard des exigences de fiabilité retenues, car la défaillance d'un macro-élément, quel qu'il soit, provoque la rupture du service téléphonique pour, au moins, tout le bâtiment concerné. Les trois autres variantes proposent une continuité satisfaisante de la fonction téléphonique, à des degrés plus ou moins élevés. En effet, la défaillance d'un macro-élément ne perturberait au maximum que la moitié des raccordements, ce qui peut être rendu tout à fait acceptable, moyennant une répartition judicieuse des raccordements de chaque macro-élément à travers les immeubles.

Cette première conclusion établie, avec l'accord de la Direction des Télécommunications de Genève, trois constructeurs de centraux ont été consultés sur la base d'un cahier des charges, décrivant l'installation souhaitée dans son intégrité, ainsi que les modalités de test en usine, de transport, de test en fin de montage, de transfert de l'ancienne installation sur la nouvelle et de fonctionnement probatoire. Les résultats de cette soumission ont permis de conclure que les solutions proposées par les trois constructeurs étaient techniquement conformes aux spécifications du cahier des charges et également homologuées par les PTT. Le Maître de l'Ouvrage a pu alors choisir en premier lieu la variante, selon les critères de disponibilité qu'il désirait. On notera ici que ce n'est pas toujours le même constructeur qui présente la solution la meilleur marché, en fonction de la variante. Dans un deuxième temps, la DBTC

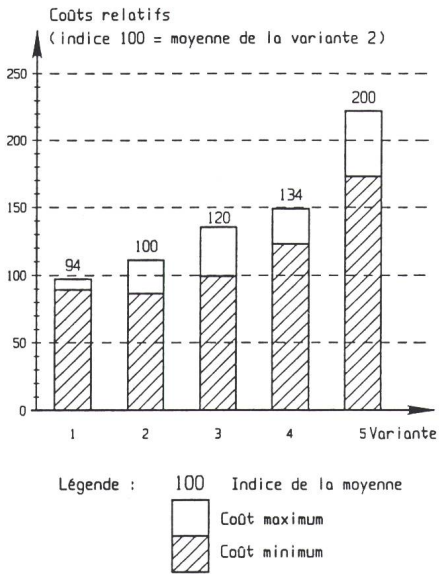


Figure 6 Récapitulatif des coûts par variante

a donc pu choisir le plus avantageux des constructeurs pour la variante qu'elle avait retenue.

On remarquera ici que l'intérêt de la variante 1 est essentiellement historique, car la notion de réseau de centraux téléphoniques est relativement récente. Par conséquent, le coefficient 100 est affecté à la variante 2. On peut noter que la variante 3 coute 1,2 fois plus que la variante de base no 2, alors qu'elle offre une quasi-sécurité (N-1). C'est la raison pour laquelle cette variante a finalement été retenue. La figure 7 montre le schéma synoptique de l'installation finale selon la variante 3.

En ce qui concerne les liaisons entre les centraux, leurs périphériques et le central public PTT, l'analyse des conséquences d'une défaillance sera limitée à deux cas extrêmes (fig. 8).

Le cas 1 illustre une rupture physique totale des liaisons inter-immeubles, donc du faisceau de trente fibres. On note que 50% des abonnés de chaque immeuble disposent normalement de leur téléphone. Le cas de la panne d'un convertisseur opto-électrique (ou, plus généralement, d'une seule fibre optique) serait moins dramatique, car il ne ferait que limiter provisoirement le nombre de canaux entre les macro-éléments, donc la capacité de trafic interne.

Le cas 2 concerne la rupture d'un faisceau de câbles PTT. Le central de l'immeuble «isolé» a la capacité de faire transiter ses appels sortants par débordement via le réseau d'ECA et l'autre central. Le central public PTT, ayant détecté la rupture de faisceau, envoie tous les appels entrants via l'autre central. La seule conséquence serait donc une limitation de la capacité de trafic externe.

De plus, le planning des PTT prévoit la mise en service prochaine d'un nouveau central de quartier à proximité de l'un des immeubles. Celà permettra alors de découpler encore mieux les deux immeubles vis-à-vis des défaillances possibles.

On relevera enfin que des tests de réception en usine ont permis de vérifier les débordements de trafic d'un central sur l'autre, ainsi que diverses autres particularités de l'installation. Ce mode de faire, courant pour les installations à courant fort, est assez rare dans le domaine des télécommunications pour être signalé.

Conclusion

L'application décrite dans le chapitre précédent montre que le choix de l'architecture d'une installation téléphonique peut modifier de façon sensible le comportement de la dite installation téléphonique en cas de macrodéfaillance, sans pour autant en accroître le prix de façon prohibitive. La valeur de la disponibilité s'en trouve sensiblement améliorée, et le critère de disponibilité exigé est respecté. La particularité intéressante de la réalisation du central téléphonique RNIS de la DBTC réside dans la possibilité qu'a eue le Maître de l'Ouvrage de choisir d'abord la variante technique, puis le constructeur, parmi ceux qui étaient capables de répondre au cahier des charges, pour un coût minimum. L'ordre habituel des choses, qui consiste à choisir un constructeur, puis à lui demander une offre pour le projet, a ainsi pu être modifié, dans le plus

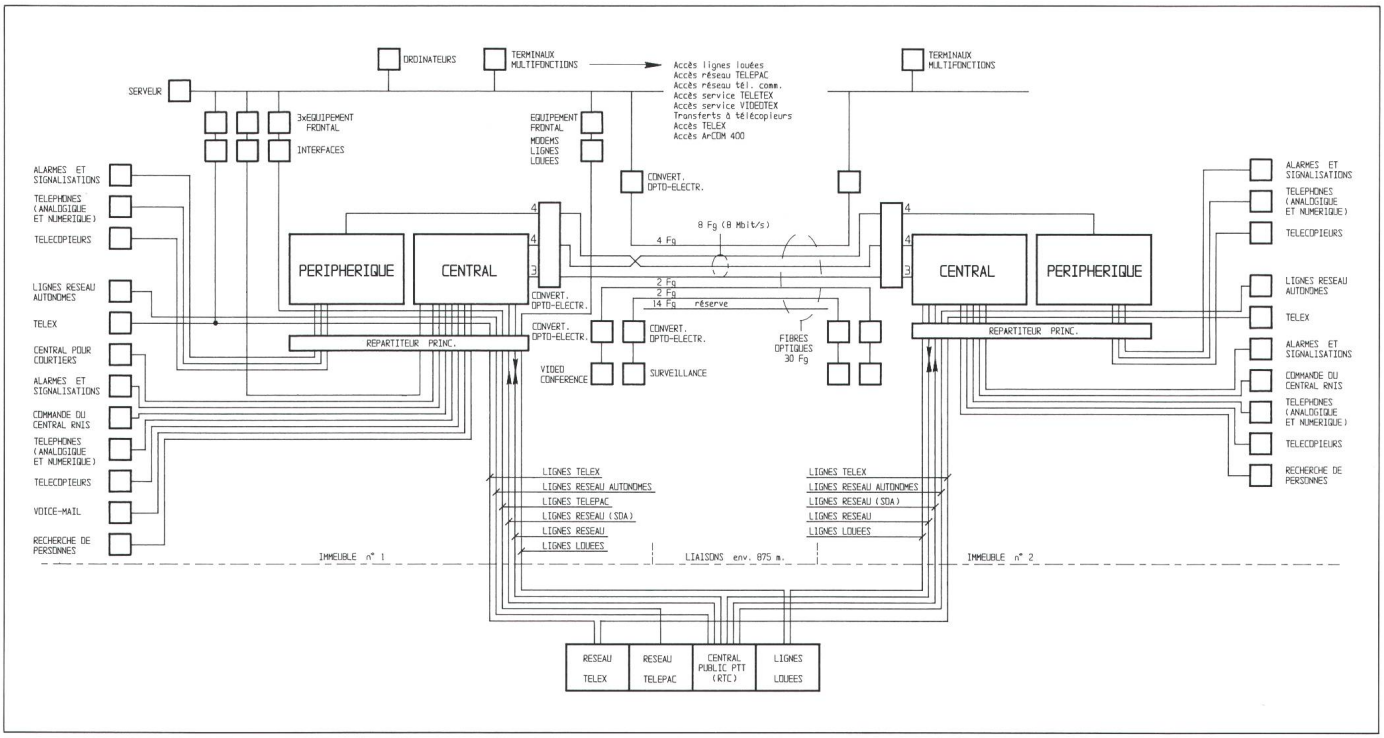


Figure 7 Synoptique de l'installation
(variante 3)

grand intérêt du Maître de l'Ouvrage.

On remarquera qu'une étude de ce genre est facilitée par l'utilisation de l'ordinateur, depuis le stade de la conception (examen rapide de plusieurs variantes) jusqu'à la réalistion des nombreux schémas d'exécution nécessaires à ce type d'installation. Parmi les tâches confiées à l'ordinateur, on trouve donc, d'une part la schématique (utilisation de CAO/DAO pour la réalisation des différents schémas de principe, d'implantation et d'installation), et d'autre part l'aide aux calculs spécifiques, tant techniques qu'économiques (utilisation de tableurs et de programmes de calculs «faits maison», écrits en langage de programmation structurée). Par exemple, l'un de ces programmes a permis d'évaluer le nombre de canaux de transmission sur fibre optique en fonction des critères particuliers de l'installation. Le matériel informatique utilisé pour cette étude est constitué d'un ordinateur IBM PS 2/80 avec écran graphique et souris, et d'un traceur graphique AO.

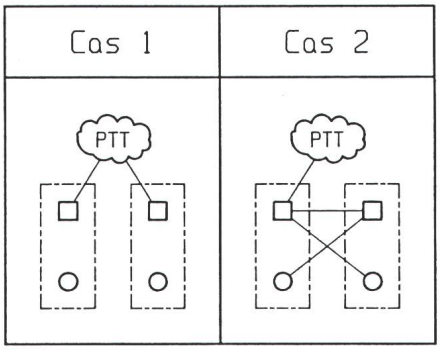


Figure 8 Défaillance des liaisons pour la variante 3