Données partagées = danger !

Travailler en partageant des données produit, c'est très bien. A condition de ne pas prendre de risques avec des informations critiques. Les outils existent, assurant la sécurité des données échangées à différents niveaux.

Désormais, le développement produit rime avec « travail collaboratif ». Mais ce n'est pas sans risque. Pour les grands acteurs, cela implique de faire sortir de l'entreprise des informations parfois critiques. Pour les petits, cela signifie d'exposer son savoir-faire à la vue de tous, voire de se le faire voler au profit d'un concurrent moins cher. Les solutions existent, depuis le minimum nécessaire jusqu'à des procédures particulièrement sophistiquées.


PTC

Contrôle du transit et des accès

Premier réflexe à avoir lorsque l'on échange des informations : contrôler l'accès aux données. Exemple avec Buzzsaw, l'outil de collaboration d'Autodesk. Arcadis, groupe international spécialisé dans la gestion de projets, s'en sert depuis 2004. « *Nous l'utilisons actuellement pour une cinquantaine de projets, pour le partage de données de façon ponctuelle en interne et le suivi de gestion documentaire pour nos clients* », commente Laurent Morisseau, responsable CAO d'Arcadis en France et Roumanie. Pas moins de 250 utilisateurs ont accès à près de 80 Go de données au travers de cet outil. Chacun accède aux informations auxquelles il a droit via un identifiant et un mot de passe qui change chaque semaine. « *Nous gérons les droits d'accès jusqu'au type de document* », assure Laurent Morisseau. Pour cela, il est cependant nécessaire au responsable CAO, qui fait aussi office d'administrateur de Buzzsaw pour l'entreprise, de disposer à chaque mise en place de projet des noms, adresses e-mails et droits pour chaque utilisateur. Pour le seconder, un administrateur de projet est désigné à chaque fois.

Pour le transfert proprement dit des données, des solutions « standard » existent également, fondées sur des voies de communication sécurisées. L'automobile,

Julien Monin, Expert Sécurité chez Avanade (JV entre Microsoft et Accenture dédiée à l'intégration de la plateforme Microsoft en entreprises)

Le système d'exploitation participe à la sécurité

Les outils de collaboration sont nombreux. Microsoft propose aussi les siens, à commencer par SharePoint et Office Communications server (OCS), qui permet de gérer la collaboration en direct, ou encore Groove, qui mêle le principe du FTP et le « peer to peer », en envoyant automatiquement une mise à jour des fichiers partagés à chaque modification.

Les logiciels utilisés par les industriels proposent des options de sécurité pour des accès directs, mais celui qui accède à la machine passe la couche de sécurité. Ainsi, un administrateur peut avoir accès à des informations qui ne le concernent pas. Ces logiciels ont donc besoin de faire de la gestion en fonction des rôles de chacun (RBAC).

En termes de sécurité, les systèmes d'exploitation jouent un rôle important et améliorer le niveau de protection. Ceux de Microsoft sont capables de prendre en charge la gestion des identités et le cryptage, par exemple.

Windows peut également établir un VPN entre deux serveurs à partir du moment où il y a un échange de fichier. Et même le mail peut être considéré comme sécurisé s'il est associé à un certificat.

Enfin, on associe souvent problème de sécurité avec échanges avec l'extérieur mais il faut se rappeler que 80% des vols de données en entreprises se vont de l'intérieur. Il est donc primordial de traiter les échanges internes avec la même rigueur que les externes.

PTC

René Iogna, consultant sénior chez MDTVISION

La collaboration doit passer par des plateformes

Le travail collaboratif consiste à regrouper des acteurs, des outils et des données sur un même espace de travail. Cela doit passer par des plateformes qui permettent d'exposer des données dédiées au travail des partenaires, mais aussi de suivre les engagements des chacun. Au niveau protection, ces environnements ne doivent pas être liées à une suite d'outils en particulier. C'est à elles de supporter la couche de sécurité. En outre, elles doivent être administrées et comporter des outils de contrôle d'identité, mais aussi inclure des mécanismes de délégation, car le donneur d'ordre n'a pas la vision de l'ensemble de la chaîne de sous-traitance. C'est ainsi au niveau N d'autoriser les accès au niveau N+1. Plus on pénètre dans la plateforme plus on trouve des informations importantes. Cela doit donc se conjuguer avec la gestion de zones au niveau de sécurité différent : une zone publique, une privée, une zone sécurisée et une dernière hautement sécurisée. Avec des règles d'accès et des filtres différents. En général, nous préconisons de travailler sur des données simplifiées comme des formats de visualisation plutôt que sur des données natives, car plus les volumes de données sont importants, plus la sécurisation est difficile à mettre en œuvre avec des temps de traitement raisonnables.

Enfin, il faut assurer la sécurité des produits, des programmes et des moyens eux-mêmes. Cela passe par des procédures et des règles d'accès strictes définies dès le départ. Lorsque les processus d'agrégation des données qui permettent de construire les vues que l'on veut partager sont verrouillés, les mécanismes d'échanges peuvent être très automatisés car c'est la couche applicative de la plateforme qui s'en charge.

par exemple, passe par des lignes ENX, complètement verrouillées. Il est aussi possible d'utiliser des réseaux privés virtuels (VPN), qui permettent d'échanger en toute sécurité entre deux sites, ou encore des lignes Internet classiques, mais cryptées.

Sécuriser la sortie des données

« Les réseaux privés préservent les données en transit. Tant que les données sont dans ce tube, elles sont protégées. Mais il faut aussi en contrôler la diffusion hors du cadre de l'entreprise », prévient Chistophe Marée, directeur marketing d'Adobe Systems France. La solution d'Adobe ? Le format PDF, bien sûr. *« Depuis notre rachat de TTF, le PDF supporte le texte, les tableurs, les images, les vidéos et les modèles 3D »*, annonce-t-il. Life Cycle, qui permet de générer les documents, dispose même de 50 filtres CAO. Dans le cadre d'une consultation, un donneur d'ordres peut donc envoyer par e-mail un dossier complet à ses sous-traitants. Ces derniers peuvent lire et annoter les documents, voire extraire des géométries exactes s'ils y sont autorisés. Et côté contrôle d'accès, le format d'Adobe va assez loin. Outre des accès par mot de passe, il peut ainsi intégrer des signatures et des formulaires qui permettent de garantir que la donnée a été lue, et de récolter une réponse directement. Mieux, *« nous utilisons la technologie de DRM (digital right management) mise au point à l'origine pour la protection des morceaux musicaux »*, explique Christophe Marée. Toute personne qui veut ouvrir le document devra alors s'identifier auprès d'un serveur de droits qui applique une politique de sécurité donnée. *« Il est alors possible de révoquer un accès à tout instant, de n'autoriser qu'une ouverture unique du document ou durant une période donnée, de verrouiller l'accès aux informations lorsque le processus de consultation a abouti, mais aussi d'avertir l'utilisateur que le document n'est plus à jour et l'inviter à télécharger la bonne version… »*, explique le directeur marketing. Concrètement, c'est le PDM de l'envoyeur qui lance des requêtes à Lifecycle à chaque modification des données concernées.

Des portails dédiés

Pour tenir compte du cycle de vie des produits, les « travailleurs collaboratifs » explorent également une autre voie : l'accès direct à une base de données commune. Dans ce domaine, *« il y a deux modes de collaboration possibles : la collaboration multi-site mais interne à l'entreprise et le partage de données avec un écosystème*, explique Olivier Meunier, Responsable avant-vente chez Siemens PLM Software. *Le premier schéma ne nécessite pas de sécurité en particulier, sauf lorsque l'on travaille dans des pays comme la Chine. Cela passe alors par des architectures techniques particulières avec un référentiel central et des données distribuées. Les équipes projets éditent les données qui peuvent être accessibles par les Chinois et on organise les synchronisations »*.

Dans le deuxième cas, là encore, plusieurs configurations sont possibles. *« Pour*

deux OEM qui travaillent ensemble, deux constructeurs automobiles qui ont décidé de partager des moteurs, par exemple, chacun travaille avec ses propres outils. Les échanges passent par un portail d'accès qui permet à l'un de réintégrer les données de l'autre dans son environnement », explique Olivier Meunier. Chacun a donc accès à la maquette numérique complète. Afin de protéger les méthodes de conception de chacun, l'éditeur propose cependant de la partager via son format de visualisation JT, qui occulte l'historique de conception.

Pour des relations donneur d'ordres/sous-traitant la solution préconisée par l'éditeur consiste à extraire les données nécessaires dans la base en les filtrant puis de constituer un « paquet de données » envoyé au sous-traitant. Il propose pour cela des outils baptisés RFx (pour request for x) intégrés dans TeamCenter. Les informations en retour sont ensuite resynchronisées par le logiciel de GDT avec la base centrale. Pour les processus de consultation, les mêmes outils servent à publier les infos dans un environnement dédié : un portail de travail collaboratif. *« Le serveur peut être devant ou derrière le fire-wall de l'entreprise, pour assurer la sécurité »*, commente Olivier Meunier. Intérêt de ce type de solution, elle est non intrusive. Or, *« souvent, les sous-traitants préfèrent ne rien avoir à installer dans leur propre système informatique »*, explique Olivier Meunier.

Découper l'information

L'offre de PTC repose sur la même philosophie de portail de collaboration sécurisé. *« Pour des partages entre des partenaires de confiance, nous avons développé ProjectLink, une solution d'échange et de resynchronisation entre un utilisateur en interne et un autre à l'extérieur »*, commente Laurent Germain. Là aussi, le processus consiste à choisir les données qui seront échangées et de créer des lots (ou paquets) de données. Pour les échanges avec des partenaires qui ne sont pas de confiance, PTC préconise l'emploi de ProductPoint, sa solution de collaboration fondée sur Microsoft SharePoint. *« Une partie de la base est envoyée au partenaire sur une base locale »*, explique le spécialiste. La synchronisation entre windchill et la base de données Sharepoint est assurée par un module baptisé PLM Connector.

Windchill assure la sécurité de tous les échanges en découpant l'information en petits morceaux. *« L'application compartimente l'information en projets ; un niveau plus fin permet également de tenir compte des objets. Ce compartimentage permet, si on structure les données par organisation (bibliothèques, produits, projets), de définir des règles de gestion des droits et des équipes pour chacun des contextes »*, commente Laurent Germain.

« Avec Windchill, la sécurité réside sur une architecture web. Mais certains clients modestes ont du mal à justifier l'implémentation d'une telle solution », reconnaît Laurent Germain.

Pour ceux-là, l'éditeur a également passé un partenariat avec Adobe qui lui permet de gérer un serveur de droits DRM associés à des fichiers Pro/E.

Vers des plateformes sécurisées

Cette notion de portail de collaboration a ouvert la voie à des espaces encore plus dédiés à la collaboration, des plateformes de collaboration, comme celles mises en place par PI3C. Problématique supplémentaire pour le prestataire de services : garantir le cloisonnement des projets les

Jean-Michel Aberide, Responsable des activités avant-ventes du département PLM d'Euriware

Le contrôle d'accès ne suffit pas

La sécurité de l'information n'est pas liée uniquement à la traçabilité mais peut aussi être portée par l'information elle-même. Ainsi, même si l'on y a pas accès, avoir connaissance de l'existence d'une donnée peut constituer une information importante. Gérer les conditions d'accès ne suffit pas. Pour assurer la sécurité, il faut morceler l'information. L'idée est de fournir à un partenaire uniquement l'information qui le concerne, lui procurer une « vue » particulière à son métier et ses habilitations. C'est une tendance forte dans l'automobile, dans le nucléaire aussi, où l'on demande des systèmes capables de masquer une information ponctuellement.

En CAO, cela est possible à travers un paramétrage fin. On peut aller jusqu'à générer une vue morte, sans intelligence. Mais une action humaine est encore nécessaire pour « déshabiller » un modèle et l'enrichir. En amont, la transformation (« enrichissement » ou « appauvrissement ») des données manque d'automatisme et si les outils de PLM ont progressé, l'intégration des outils nécessaires n'est pas complète. En outre, plus a besoins de découper finement, plus il faut se gratter la tête pour définir les bons critères et chaque cas est différent.

Gilles Battier, P-DG de Spring Technologies et responsable du groupe « travail collaboratif du pôle de compétitivité System@tic.

Le cas des projets de R&D

Les travaux de sous-traitance font de plus en plus appel au travail collaboratif, mais il ne faut pas oublier les projets de R&D lancé par plusieurs entreprises. Dans ce domaine, la sécurité des informations est importante lors des contacts avec l'extérieur, mais aussi en interne car les PME ont souvent peur de se faire dépouiller de leur savoir-faire. A System@tic, nous recommandons la signature d'une convention dont nous avons créé un modèle. Le document fait 50 pages et prend en compte tous les aspects. Dans ce type de projet, la sécurité passe aussi par un bon choix de partenaires complémentaires et le moins concurrents possibles. Quant aux échanges d'informations, lors des revues, par exemples, ils peuvent passer par des « démonstrateurs ». Il s'agit alors de montrer le résultat des recherches, mais pas la technologie qu'il y a derrière. Mais ce n'est pas toujours évident. Enfin, le partage par un dispositif de type FTP n'est pas forcément une erreur. Car même si elles sont accessibles, les informations ne sont pas toujours utiles si on ne sait pas les remettre dans le bon ordre.

uns par rapport aux autres, car ils peuvent concerner des entreprises concurrentes. *« Nous appliquons deux couches de sécurité : la nôtre et celle des hébergeurs IBM et Exanet. Côté PI3C, la protection est assurée par projet, par personne et par organisation »*, assure François Tribouillois, PDG de l'entreprise. En outre, les modes d'affichage peuvent être adaptés. *« Quand on publie les pièces dans Solidworks par exemple, on peut effacer une pièce ou une partie d'une pièce pour recréer un « modèle commercial ». On isole des zones du modèle et on ne donne accès qu'à certaines »*, explique le chef d'entreprise. Une solution intéressante pour les spécialistes de l'implémentation d'usines qui peuvent ainsi partager une partie seulement du site avec tel ou tel partenaire.

Le mode on-line est plus sûr

Chez Dassault Systèmes, la V6 est elle aussi construite autour de cette notion de plateforme. Elle autorise deux modes de travail : connecté (synchrone ou asynchrone), via 3DLive, ou déconnecté (par échanges successifs de données). *« Le mode connecté, ou on-line, permet d'avoir des données à jour à tout moment. Dans ce cas, nous assurons la gestion d'autorisations d'accès à un niveau standard, avec des identifiants et mots de passe, ou à un niveau renforcé, par exemple avec des certificats »*, explique Stéphane Declée responsable des solutions On Demand Enovia chez DS. La plateforme assure ainsi une gestion des accès par identité, mais aussi par rôle dans un projet.

Pour le spécialiste, le mode online est plus sûr qu'une solution qui oblige à sortir des données du cadre de la plateforme. D'autant que les informations échangées dans 3DLive sont des informations de rendu. Et pour renforcer la sécurité, *« nous assurons également une gestion très fine des données PLM. Les informations sont filtrées à plusieurs niveaux, du paquet entier à l'objet seul. Il est possible de définir que telle personne n'a pas accès à tel type d'objet voire à tel objet »*, détaille Stéphane Declée. L'éditeur peut aussi associer des mécanismes de DRM ou certificats aux données exportées. En outre, *« le système n'envoie que les données modifiées. Cela assure des temps d'itération très courts »*, explique Stéphane Declée. Et surtout, *« les informations ne sont utilisables que dans le cadre de deux (ou plus) V6 qui communiquent ensembles »*, poursuit-il. La démarche permet d'améliorer la performance du système, car tout dispositif de sécurité, en particulier le cryptage, risque d'avoir une incidence forte sur la vitesse des opérations. Et puisque les échanges ne concernent que des informations partielles, les capter à la volée ne servirait pas beaucoup à un éventuel pirate…

Il reste encore des axes de travail à affiner, notamment lors de la configuration. Par exemple, simplifier la définition des droits d'accès avec des modes de sélection multicritères plutôt que par la sélection manuelle de chaque objet… En outre, *« la technologie est sûre, mais certains utilisateurs ont encore des réticences à travailler en mode « connecté » »*, reconnaît Stéphane Declée.

Attention aux hommes

Pour François Tribouillois, *« les problèmes informatiques liés à la sécurité des données sont facile à régler. Mais si les méthodes de travail ne sont pas bonnes, même avec de bons outils, on ne peut pas arriver à de bons résultats »*. Si certaines entreprises mettent un soin particulier dans la sécurisation des mouvements de leurs données, *« elles oublient parfois le maillon le plus important de la sécurité : l'humain »*. Laisser un fichier ouvert alors qu'on s'absente de son poste, envoyer des informations par e-mail ou les mettre à disposition sur un FTP… le comportement des utilisateurs eux-mêmes est souvent plus dangereux pour l'entreprise que les transferts informatiques. Cela peut valoir la peine de s'interroger sur ces questions avant d'investir de l'argent et de l'énergie dans un outil de collaboration ultra pointu. ■

Trois industriels accros à la sécurité

Segula s'adapte à tous les cas

Pour Segula Technologies (6500 personnes, plus de 500 millions € de chiffre d'affaires en 2008), le métier d'ingénieriste est en pleine évolution. En quelques années, le groupe est ainsi passé d'un schéma d'assistance technique chez ses clients à la globalisation de projets externalisés dans ses locaux. Autrement dit la prise en charge d'une activité complète, par exemple le calcul ou le développement global d'une partie d'un véhicule automobile pour le compte d'un donneur d'ordres. Dans certains cas, cette externalisation aboutit au montage d'un plateau dans le Bureau d'études exclusivement dédié au client de Segula.

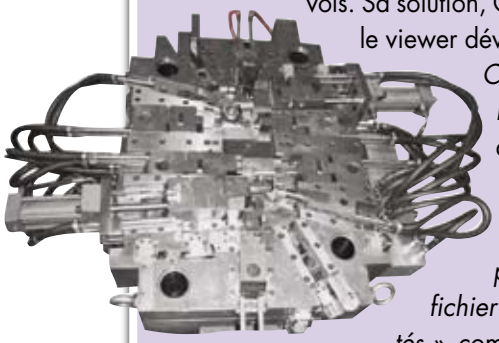
A chaque configuration correspond un dispositif de sécurité adapté. *« Lorsque les données que nous manipulons restent chez le client, nous respectons ses propres règles de sécurité, validées lors d'audits. Pour celles hébergées sur nos sites, nous appliquons nos consignes internes. L'application de ces consignes est en outre auditée en interne »*, déclare Iscliff Lebee, responsable ingénierie numérique et collaborative du département automobile. Quant aux échanges d'informations, de plus en plus fréquents entre ses 70 sites et ceux de ses clients, Segula propose plusieurs solutions. Quand le donneur d'ordres impose son dispositif, une zone informatique dédiée (ZID) et un portail accessible au travers d'un réseau privé (VPN) sont mis en place, avec l'appui de lignes sécurisées. Quand le client ne dispose d'aucune solution sécurisée, l'ingénieriste propose une prestation complète utilisant des outils dédiés : un portail web réalisé à partir de EDTi de Numlog, ainsi qu'un visualisateur et un outil de conférence à distance pour faciliter le travail collaboratif.

« En règle générale, ce sont plus de 6 000 références (techniques et relatives au projet) client qui sont utilisées à chaque projet », annonce Iscliff Lebee. Segula doit alors assurer la sécurité des échanges, mais également leur confidentialité, leur traçabilité et leur sauvegarde pour permettre au client de conserver l'historique de chaque projet. Pour cela, l'ingénieriste a inséré un niveau de protection supplémentaire : les échanges entre Segula et ses donneurs d'ordres passent par un outil spécifique baptisé Segula Protection System (SPS), qui assure le lien avec sa solution PDM interne. Ce système construit autour de SmartTeam, de Dassault Systèmes, administre également la gestion des accès pour tous les effectifs affectés au projet, quels que soient les délais de participation.

La définition du niveau de criticité des données, la configuration du VPN et la circulation des informations dans le cadre du projet sont gérées de façon stricte par un petit nombre de personnes désignées au départ. *« Tout cela permet d'uniformiser les projets et d'assurer la sécurité et la confidentialité par projet et par client »*, souligne Iscliff Lebee. Et Segula compte aller encore plus loin. *« Un des points complexes est de savoir comment faire transiter toutes les informations associées aux données entre des PDM différents »*. L'ingénieriste vient d'ailleurs, d'ouvrir sur ce sujet un projet interne de « Recherche et Innovation » afin de compléter son offre.

Georges Pernoud communique via un viewer

Georges Pernoud, à Oyonnax (Ain), est mouliste. L'entreprise qui emploie 80 personnes possède trois entités, dont une en Slovaquie. Sa problématique est simple : avec près de 800 demandes de devis par an, elle doit pouvoir visualiser et traduire rapidement les données de ses donneurs d'ordres en format compréhensible par Think-Design (son outil de conception), mais aussi faire sortir des informations de l'entreprise sans crainte de fuites ou de vols. Sa solution, Gilles Pernoud, co-dirigeant de l'entreprise l'a trouvée il y a deux ans : WorkXplore3D, le viewer développé par Sescoi. *« A chaque consultation, nous ouvrons les fichiers avec le viewer. Cela évite de traduire le format d'origine pour une affaire qui ne nous convient pas. Si nous voulons prendre l'affaire, nous exportons le fichier en Iges »*, explique le chef d'entreprise.



Pour Pernoud, ce petit outil est aussi synonyme de sécurité. *« Pour faire nos demandes à des fournisseurs d'éléments de moules, nous envoyons un exécutable qui leur permet de visualiser les pièces et d'y effectuer des mesures, mais pas d'extraire le fichier CAO. Désormais, nous envoyons ainsi des données en Chine sans stress d'être piratés »*, commente Gilles Pernoud. De la même façon, lorsqu'il présente ses résultats à ses clients, l'industriel utilise le viewer. Il est alors possible de visualiser le produit, éventuellement au travers d'animations, et même de laisser un exemplaire sur place sans crainte que les informations soient récupérées par un autre mouliste. Enfin, *« nous l'utilisons également pour communiquer avec nos collègues slovaques. Nous pouvons nous envoyer des données importantes sans dispositif ultra-sécurisé »*, annonce Gilles Pernoud. Sans compter que les fichiers sont alors souvent cent fois plus légers que des modèles CAO. Et outre la sécurité, *« l'outil 3D est très important en communication. Tout le monde comprend plus vite »*, poursuit-il. Au point que ses 16 licences flottantes de WorkXplore3D sont désormais également utilisées à l'atelier et par les commerciaux.

Bourbon Fabi crée son propre portail

Bourbon Automobile, filiale du petit groupe international Bourbon Fabi, est spécialisée dans la fabrication de pièces d'intérieur (poignées de portes, pommeaux de levier de vitesse, insignes…) pour l'automobile. Avec ses donneurs d'ordres, l'entreprise de Saint-Lupicin (Jura) se plie aux exigences en rigueur. *« Les consultations passent souvent par un portail spécifique dans lequel est placé le cahier des charges de consultation constitué de différents documents aux formats Word, PDF, Excel ou JT (le format de visualisation de Siemens PLM Software)… »*, explique Christian Genez, directeur de l'organisation des systèmes d'information. L'entreprise reçoit par mail son login et son mot de passe et peut faire son offre. Si elle est retenue, elle est généralement redirigée vers un autre portail dédié au développement contenant davantage d'informations. *« A part une ligne internet ou une ligne spécialisée et un peu de compétences en informatique, on n'a besoin de rien de particulier »*, assure Christian Genez. Le sous-traitant a ainsi accès très tôt à des informations et des métadonnées critiques, les noms des futurs véhicules et des modèles natifs complets de sous-ensembles, par exemple. Mais il doit se conformer aux contrats de confidentialité globaux et particuliers signés avec ses clients. Dans l'autre sens, l'entreprise protège son travail en envoyant, quand c'est possible, des « solides morts ». *« Ce sont des modèles 3D dont les pièces ne peuvent être dissociées »*, explique le directeur. Mais cela prend du temps…

Depuis peu, Bourbon Fabi a mis en place un dispositif analogue, mais pour ses 200 fournisseurs. *« Nous avons créé un portail auquel ils se connectent via un accès Internet classique »*. Ce portail créé avec Numlog contient des informations issues de son logiciel de PDM qu'ils n'ont plus qu'à venir piocher. Points particuliers de ce système : d'abord les données ont une durée de vie limitée et sont détruites après téléchargement. Ensuite, pour éviter tout risque d'erreur, Bourbon n'envoie que des numérisations complètes et le logiciel de PDM génère à chacune de leur modification un fichier Excel qui permet d'identifier la « bonne version ». Enfin, *« la gestion des accès est directement gérée par le PDM qui synchronise un carnet adresse Outlook avec celui du portail »*, explique Chritain Genez. Désormais, l'entreprise envisage de faire transiter plus d'informations via le portail, les bons de commandes et les comptes-rendus d'essais de moule, par exemple.