

Projet BOUM

Maquette d'interface utilisateur sécurisée

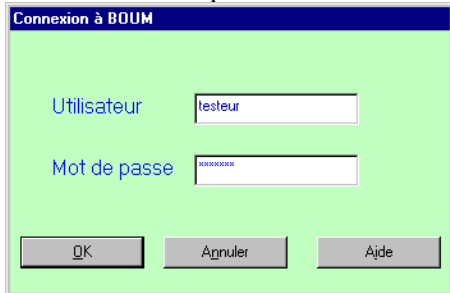
Régis Lécu, 07/07/2016, annexe de la séance « Sécuriser l'interface utilisateur »

Sommaire

1.	<i>Authentification et droits</i>	3
2	<i>Partie bureautique</i>	6
2.1	Les maquettes d'écran et les comportements type	6
2.2	Normalisation des vérifications et des messages d'erreur	7
2.3	Maquettes des écrans (extrait)	8
3	<i>Partie contrôle (extrait)</i>	13

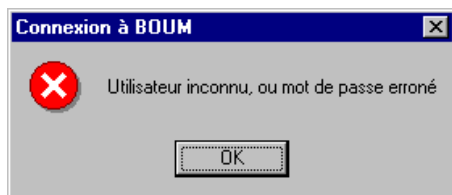
1. AUTHENTIFICATION ET DROITS

La partie bureautique de l'application BOUM débute par une feuille de connexion qui demande le nom et le mot de passe d'un utilisateur autorisé :



L'utilisateur peut valider sa saisie en cliquant sur « OK » ou abandonner l'application en cliquant sur « Annuler ».

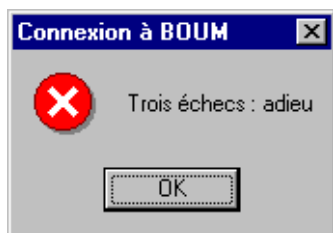
Si le nom ou le mot de passe saisis sont invalides, l'application prévient l'utilisateur par un message d'erreur :



(Contrôler ses sorties : message d'erreur fonctionnel sans information technique, qui ne précise pas la cause de l'erreur (utilisateur / mot de passe), pour ne pas donner d'indice à un attaquant)

Au bout de trois essais infructueux, l'application s'arrête avec le message d'erreur :

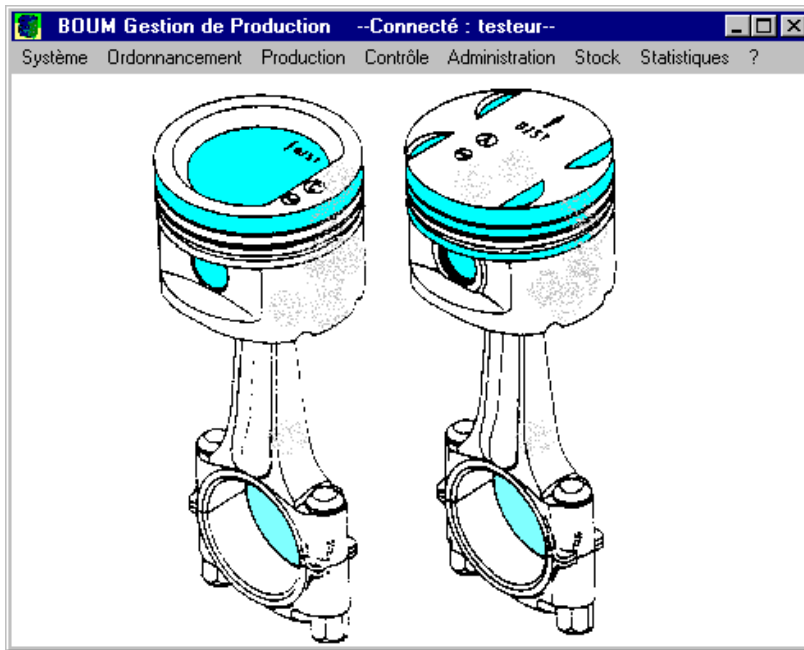
(Pour décourager une attaque de compte utilisateur par « force brute »)



Si la connexion réussit, l'utilisateur accède à une fenêtre principale avec une barre de menu : seuls seront visibles les menus qui correspondent à des fonctionnalités autorisées pour cet utilisateur.

Par souci de clarté, l'application affiche l'état courant (**Connecté**) dans sa barre de titre. Pour éviter une erreur à un utilisateur de bonne foi, elle précise aussi le nom de l'utilisateur connecté (**testeur**).

Les menus **Système** et **?** seront accessibles par tout le monde, dans l'état connecté ou déconnecté.



Les menus ne seront tous visibles que pendant la phase de développement, en compte de test.

Le menu et la fonctionnalité de **Contrôle** ne seront accessibles que pendant la phase de développement, et seront déployés dans une application dédiée à **l'Atelier**.

Liste des fonctionnalités permises par type d'utilisateur

En vert : les options toujours accessibles

En orange : l'application d'atelier pour le Contrôle des pièces

En bleu : l'application bureautique pour l'administration et le magasin

Menu	Sous-Menu	Fonctionnalité autorisée	Utilisateur
Système	Connexion	Pour se connecter sous un autre compte utilisateur	Tout le monde
	Quitter	Pour quitter l'application	Tout le monde
Ordonnancement	Consulter le stock	Visualiser l'état des stocks et des ruptures	Resp. Atelier
	Lancer un lot	Lancer un lot, suite à une rupture de stock	Resp. Atelier
Production	Démarrer un lot	Démarrer la production, en affectant le lot à une presse disponible	Resp. Production
	Terminer un lot	Terminer la production du lot, et libérer la presse	Resp. Production
	Visualiser les lots	Visualiser l'état courant des lots	Resp. Production
Contrôle	Saisir les côtes	Saisir les côtes d'une nouvelle pièce	Contrôleur
	Clôturer un lot	Terminer le contrôle d'un lot	Contrôleur
Administration	Machines	Sous-menus de création et suppression d'une presse	Resp. Application
	Modèles	Sous-menus de création et suppression d'un modèle	Resp. Application
	Définir Seuil mini	Saisie du seuil minimum d'un stock	Magasin
Stock	Mouvement	Entrée ou sortie de stock	Magasin
Statistiques	Réduites	Totaux et stat, par lot	Resp. Qualité
	Détaillées (par lot)	Courbe par lot	Resp. Qualité
?	A propos de	Feuille de version et d'aide	Tout le monde

Remarques sur la sécurité :

L'interface utilisateur n'affiche pour chaque utilisateur que les fonctionnalités autorisées, ce qui constitue un premier niveau de défense.

Mais l'application protégera également les données côté serveur, par les autorisations affectées aux tables et aux procédures stockées (défense en profondeur, deuxième niveau).

Sécuriser l'interface utilisateur : maquette d'interface sécurisée

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

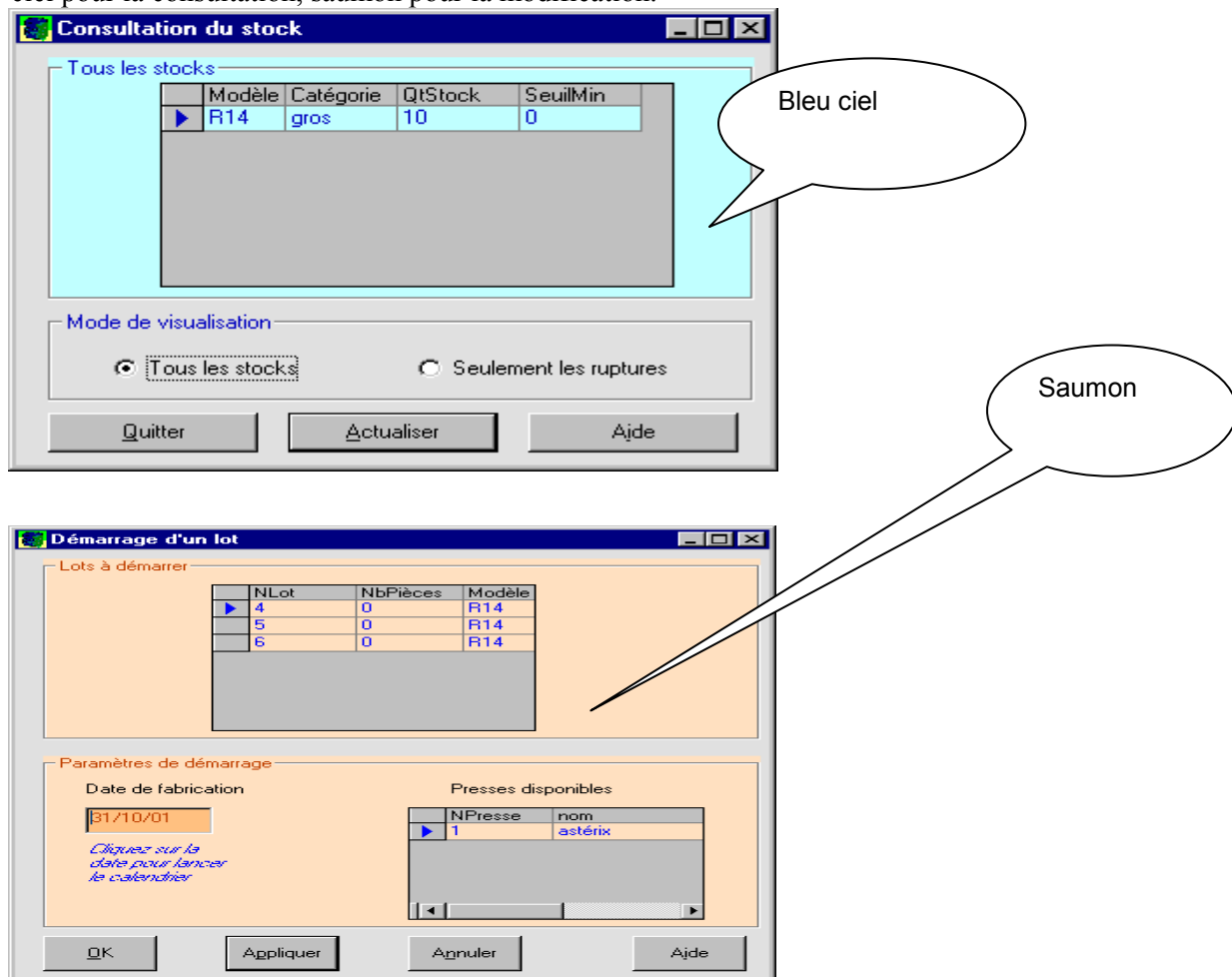
2 PARTIE BUREAUTIQUE

Les choix d'ergonomie décrits dans les maquettes d'écran répondent à deux objectifs :

- ils facilitent la tâche de l'utilisateur normal, en limitant les possibilités d'erreurs.
- ils compliquent la tâche d'un attaquant, en réduisant autant que possible l'exposition des données et l'accès aux fonctionnalités.

2.1 Les maquettes d'écran et les comportements type

Notre ergonomie est définie par les maquettes ci-dessous, qui suivent une charte des couleurs : bleu ciel pour la consultation, saumon pour la modification.

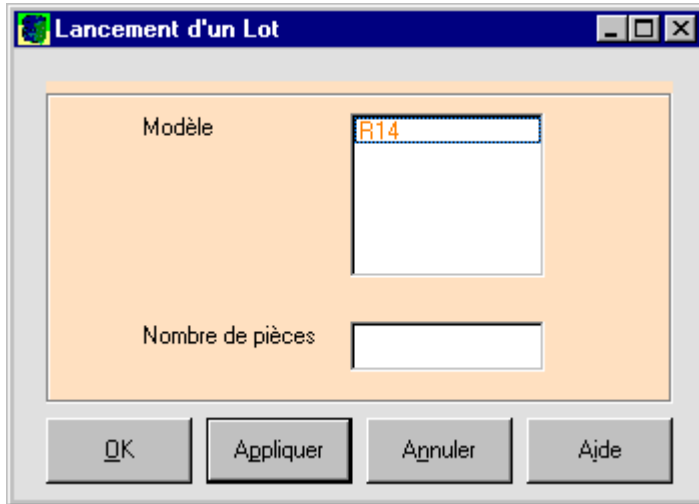


a) Les écrans de consultation

- Les écrans de consultation (« Consulter le stock », « Visualiser les lots », « Statistiques réduites ») ne sont pas modaux : ils peuvent être ouverts en même temps que la fenêtre principale.
- Ils comportent un bouton **Quitter** pour fermer la fenêtre et revenir à la fenêtre principale, et un bouton **Actualiser** qui provoque le réaffichage des informations demandées.

b) **Les écrans de mise à jour**

- Les écrans de mise à jour sont modaux. (*Pour interdire à l'utilisateur de lancer plusieurs mises à jour en même temps*)
- Ils possèdent tous un bandeau standard avec quatre boutons : **OK**, **Appliquer**, **Annuler**, **Aide**



- **Appliquer** effectue l'action demandée sur la base de donnée côté serveur et actualise les affichages si nécessaire. Il ne ferme pas la fenêtre et permet donc des opérations répétitives.
- **OK** procède comme **Appliquer**, mais il ferme la fenêtre et revient à la fenêtre principale, en cas de réussite de l'opération demandée.
- **Annuler** ferme la fenêtre et revient à la fenêtre principale, sans effectuer d'opération.
- Tous les écrans, de consultation ou de mise à jour, comportent un bouton **Aide** qui est toujours en bas et à droite de l'écran.
- L'application ne comprend pas d'enchaînement complexe : aucune fenêtre ne lance de fenêtre fille ; une même fenêtre n'est jamais utilisée pour plusieurs objectifs, tels que la suppression et la création.

(« *Keep UI Small and Simple* »)

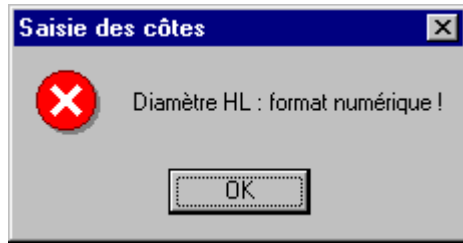
2.2 Normalisation des vérifications et des messages d'erreur

L'utilisateur peut renseigner les champs dans l'ordre qu'il désire, mais tous les champs obligatoires doivent être remplis au moment de la validation par les boutons **OK** ou **Appliquer**.

- *L'interface utilisateur vérifie donc que tous les champs obligatoires sont remplis lorsque l'utilisateur valide sa saisie.* S'il reste des champs obligatoires non renseignés, le logiciel affiche un message d'avertissement rappelant le nom du champ vide :



- *Par contre, les vérifications de cohérence sont effectuées au fur et à mesure, lorsque l'on quitte un champ.* Un champ non renseigné ne provoque pas d'erreur. Si le dernier champ saisi est incohérent, le logiciel affiche un message d'erreur, rappelant le format à saisir :



- Les messages d'erreur et d'avertissement se distinguent par leur icône (triangle jaune ou croix sur fond rouge) conforme aux Guide de style Windows, et ils portent toujours le titre de la fenêtre qui les affiche (« Saisie des côtes » dans l'exemple ci-dessus)
- Seule exception à la vérification des champs : click sur les boutons **Annuler** ou **Quitter**. L'utilisateur pourra toujours annuler son action et revenir au menu principal, même si le dernier champ saisi est incohérent.

2.3 Maquettes des écrans (extrait)

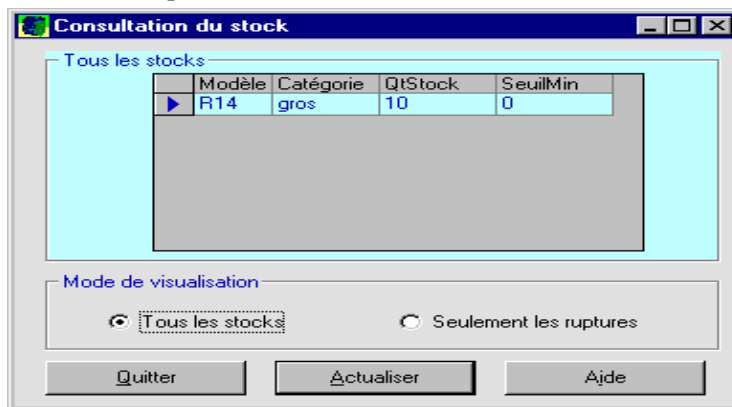
⇒ Menu **Système** : accessible à tous les comptes utilisateurs.

Le sous-menu **Connexion** permet de se connecter sous un autre compte utilisateur : *une fois dans l'écran de connexion, l'utilisateur ne peut plus revenir à sa connexion courante.* Il ne peut que valider la nouvelle connexion (bouton **OK**) ou quitter l'application (bouton **Annuler**)

Le sous-menu **Quitter** et la croix en haut à droite permettent de quitter l'application, en fermant toutes les fenêtres.

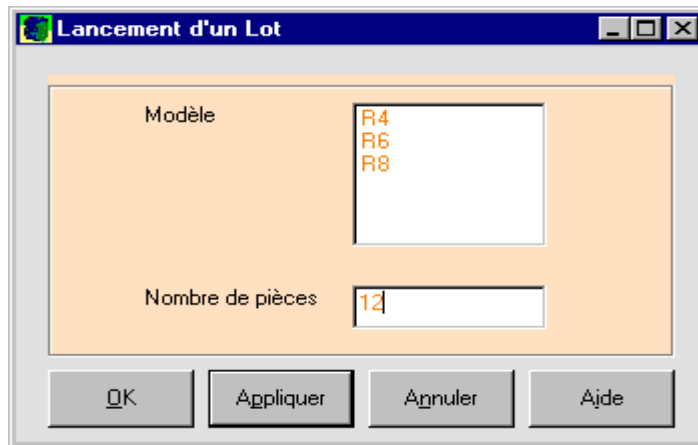
⇒ Menu **Ordonnancement** : accessible aux comptes utilisateurs du groupe **Atelier** (responsable d'atelier et son adjoint).

Le sous-menu **Consulter le Stock** affiche l'écran **Consultation du stock** qui permet de visualiser soit la totalité des stocks, soit les stocks en rupture. Pour chaque type de stock, on affiche le nom du modèle, la catégorie, la quantité en stock et le seuil minimum requis. Cet écran n'est pas modal et peut rester ouvert pendant le fonctionnement de l'application : il peut être rafraîchi par le bouton **Actualiser**.



(Ergonomie : on aide l'utilisateur normal dans son métier en lui permettant de visualiser tout le stock ou seulement les ruptures ; on limite les attaques possibles en ne permettant que la consultation, la modification étant réservée au magasinier)

Le sous-menu **Lancer un lot** affiche l'écran **Lancement d'un lot** qui permet de lancer un lot correspondant à un modèle donné, pour une quantité donnée.



Cet écran est modal.

La validation par les boutons **OK** ou **Appliquer** appelle le traitement côté serveur.

Contrôle en saisie :

Le nombre de pièces doit être un entier strictement positif.

(Validation systématique des entrées : champ texte typé avec un masque n'autorisant que les entiers positifs, pour prévenir les erreurs de saisie le plus vite possible).

Contrôles et opérations côté serveur :

Le traitement serveur vérifie que le modèle existe encore : du fait du fonctionnement en client/serveur, il aurait pu être détruit par un autre client, pendant l'affichage de la liste.
(« Défense en profondeur » à deux niveaux : interface utilisateur et traitement serveur).

Si tout est correct, le traitement serveur crée un nouveau lot, et l'interface utilisateur affiche son numéro :



=> Menu **Production** : accessible aux comptes utilisateurs du groupe **Production** (responsable de production et son adjoint)

Le sous-menu **Démarrer un lot** affiche l'écran **Démarrage d'un lot** qui permet d'affecter un lot planifié à une presse disponible.

Démarrage d'un lot

Lots à démarrer

	NLot	NbPièces	Modèle
▶	3	1200	R6
	4	12	R4
	5	121	R6
	6	12	R6
	7	12	R6

Paramètres de démarrage

Date de fabrication: 05/11/01
Cliquez sur la date pour lancer le calendrier

Presses disponibles

NPresse	nom

Buttons: OK, Appliquer, Annuler, Aide

Cet écran est modal.

L'utilisateur doit d'abord sélectionner un lot à démarrer en cliquant sur une ligne dans le cadre d'en haut, puis sélectionner une presse disponible dans le cadre d'en bas.

(Validation systématique des entrées : utilisation de composants graphiques spécialisés dans l'interface utilisateur, pour prévenir les erreurs de saisie et les attaques, sur les numéros de lots et de presse)

La date de fabrication proposée par défaut est la date système du jour. L'utilisateur peut la modifier en cliquant sur le champ date, pour lancer un calendrier :

Date de fabrication

Novembre 2001 | Novembre | 2001

Lun	Mar	Mer	Jeu	Ven	Sam	Dim
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

En sortie du calendrier, la nouvelle date sélectionnée s'affiche dans le champ **Date de fabrication**.

(Validation systématique des entrées : utilisation de composant graphique spécialisé pour prévenir une erreur de saisie ou une attaque sur la date)

La validation par les boutons **OK** ou **Appliquer** appelle le traitement serveur.

Contrôles d’affichage : seuls sont affichés les lots dans l’état « lancé » et les presses disponibles, au moment où on affiche la fenêtre

(Limitation de l’exposition des données, pour prévenir les erreurs et les attaques : on n’affiche que les presses disponibles et les lots à démarrer)

Contrôles et opérations côté serveur : le traitement serveur vérifie à nouveau que le lot et la presse existent, et sont dans un état cohérent au moment de la demande.

(Défense en profondeur : dans une application client/serveur, une donnée peut avoir été modifiée entre temps par un autre client, et il est toujours nécessaire de la revalider côté serveur).

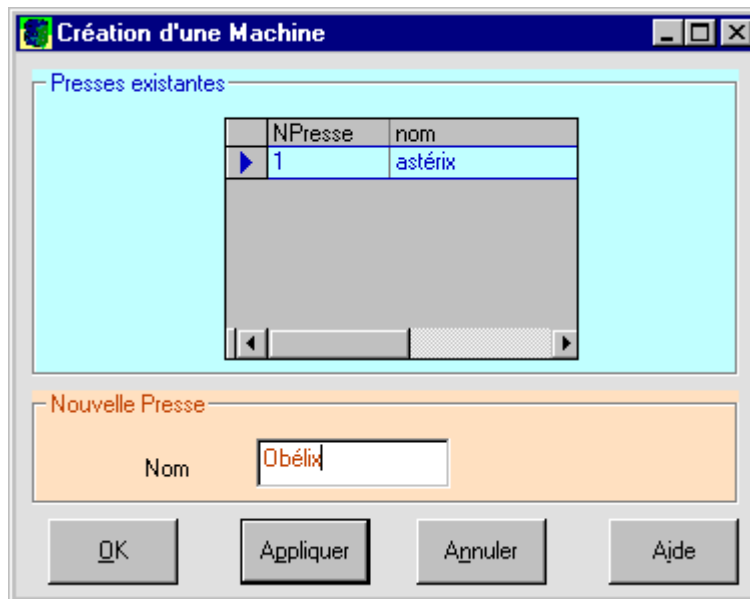
⇒ Menu **Administration** : accessible aux comptes utilisateurs du groupe **Application** (responsable de l’application et ses adjoints)

(« Keep UI Small and Simple ». Simplicité volontaire de l’interface utilisateur : formulaires différents pour chaque objet à manipuler et chaque type d’action (création, suppression))

Le sous-menu **Machines/Créer** affiche l’écran **Création d’une machine**.

Cet écran est modal.

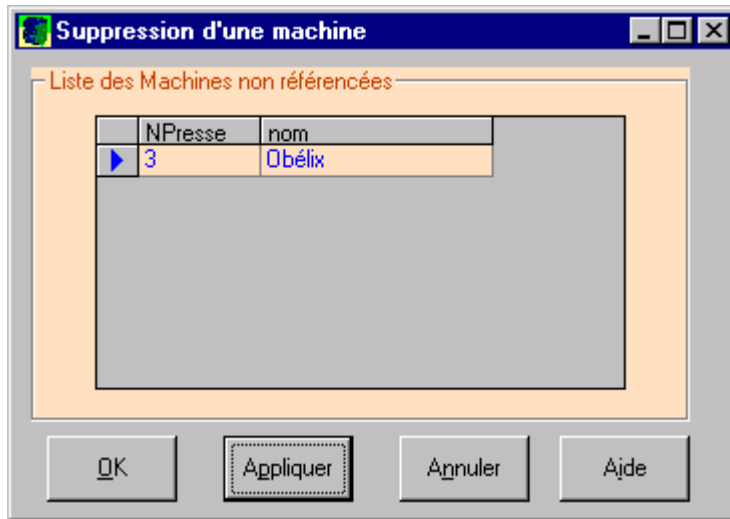
La liste des **Presses existantes** est affichée à titre indicatif. A la création d’une nouvelle presse par le bouton **Appliquer**, le nom de la presse s’affiche immédiatement dans le cadre du haut.



(Champ texte pour la nouvelle presse : on est dans le cas où aucun composant graphique spécialisé ne convient)

Le sous-menu **Machines/Supprimer** affiche l’écran **Suppression d’une machine**.

Cet écran est modal.



(Validation systématique des entrées : utilisation d'un composant graphique spécialisé (liste) pour choisir la presse à supprimer, afin d'éviter les erreurs de saisie et de limiter les attaques. Limitation de l'exposition des données : on n'affiche que ce qui peut être détruit, pour ne pas tenter les hackers)

Contrôles d'affichage :

Le cadre du haut n'affiche que les machines qui n'ont jamais été utilisées et qui peuvent donc être supprimées. Pour supprimer une machine, l'utilisateur doit cliquer sur la ligne correspondante, et valider la suppression par les boutons **OK** ou **Appliquer**.

Contrôles et opérations côté serveur : le traitement serveur vérifie à nouveau que la machine existe et qu'elle n'a jamais été utilisée.

3 PARTIE CONTROLE (EXTRAIT)

Cette partie est dédiée au travail dans l'atelier : elle commence comme la partie bureautique par une étape d'authentification, mais les seuls utilisateurs autorisés sont ceux du groupe **Contrôle**. Une fois connecté, le contrôleur ne dispose que des menus : **Système**, **Contrôle** et ?

(« Keep UI Small and Simple » :

L'application d'atelier ne doit contenir que le traitement du Contrôle, afin d'éviter toute attaque sur la partie bureautique, même en cas de compromission des comptes utilisateur.

Une séparation physique des tâches est toujours plus sûre qu'une simple protection par authentification.

Mais l'authentification reste nécessaire pour interdire aux autres utilisateurs de l'usine, ou à un attaquant, d'utiliser l'interface utilisateur du Contrôleur.

(« Usable Security » :

Parallèlement à l'effort de sécurisation, la partie Contrôle tient compte des besoins de l'utilisateur normal, en adoptant une ergonomie d'atelier, adaptée à une tâche effectuée à la chaîne, par un opérateur non informaticien.)

Le sous-menu **Saisir les côtes** de **Contrôle** affiche l'écran modal ci-dessous ;

CLiquer pour sélectionner le lot à mesurer			
NLot	NPresse	Modèle	DateFabrication
9	1	R14	07/11/01

LOT en cours de mesure ??

Vos Mesures

Diamètre HL Diamètre HT

Diamètre BL Diamètre BT

☐ Rebut

Caractéristiques de la nouvelle pièce

N° Pièce Catégorie

OK Appliquer Annuler Aide

Contrôles d'affichage : seuls sont affichés les lots en cours de mesure (dans l'état « démarré » ou « libéré »), au moment où on affiche la fenêtre.

(Utilisation d'un composant graphique spécialisé (liste) pour choisir le lot à mesurer : on évite les erreurs de saisie et on limite les attaques ; limitation de l'exposition des données : on n'affiche que les lots qui peuvent être réellement mesurés)

Sécuriser l'interface utilisateur : maquette d'interface sécurisée

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Contrôles de saisie :

L'utilisateur doit commencer par sélectionner un numéro de lot à mesurer, en cliquant sur la ligne correspondante dans le cadre du haut : le numéro de lot choisi apparaît dans le champ **LOT en cours de mesure** (à la place des ? ?)

Si l'utilisateur valide sa saisie sans choisir le numéro de lot, le logiciel affiche le message :



Les 4 côtes saisies (**Diamètre HL**, **Diamètre HT** etc.) doivent être des réels strictement positifs.
(Utilisation de champs typés avec un masque de saisie n'autorisant que les réels positifs)

Si la pièce est déclarée mesurable (case **Rebut** non cochée), les quatre côtes sont obligatoires : la vérification de remplissage des 4 champs est faite au moment de la validation.

Si la pièce est déclarée non mesurable (case **Rebut** cochée), aucune saisie n'est nécessaire (elle n'aurait d'ailleurs pas de sens)

Contrôles et opérations côté serveur :

Le traitement serveur associé gère les problèmes client/serveur en vérifiant à nouveau que le lot à laquelle la pièce est associée, existe encore et qu'il est dans un état cohérent au moment de la demande. *(« Défense en profondeur » à deux niveaux)*

Si le traitement côté serveur réussit, l'interface utilisateur affiche le numéro et la catégorie de la nouvelle pièce, pour que le contrôleur puisse la ranger dans la caisse correspondante.