Étude de cas	APPROFONDIR LA CULTURE TECHNOLOGIQUE	**Durée : 1 h 30**
	Support : SERRURE BIOMÉTRIQUE	

Nom de l'élève :	**Classe :**	**Date :**

Matériel ressource :	**Documents ressources :**
• **Serrure biométrique**	• **Livre Sciences de l'Ingénieur** • **Dossier technique de la serrure** • **Diaporama « Approche externe des systèmes »**

Compétences abordées :
- Caractériser les fonctions d'un système technique.
- Identifier des contraintes associées à une norme ou à une réglementation.
- Identifier la dimension sensible ou esthétique (design ou architecture) associée à un système, un habitat ou un ouvrage

1.Mise en œuvre de la serrure biométrique :

En suivant les procédures indiquées dans le dossier technique, réalisez sur la maquette les manipulations suivantes :

- *Essayez d'ouvrir la porte à l'aide du lecteur d'empreinte ou du clavier codé. Que constatez-vous ?* Sans code ni empreinte valide, la béquille tourne dans le vide. Il est impossible d'ouvrir la porte.
- *Saisissez, pour un ou plusieurs membres du groupe, un code et/ou une empreinte de l'index droit.*
- *Essayez de nouveau d'ouvrir la porte à l'aide du lecteur d'empreinte ou du clavier codé. Que constatez-vous ?* Maintenant, il est possible d'ouvrir la porte soit à l'aide du code, soit à l'aide de l'empreinte. Après le bip sonore, on dispose de quelques secondes pour abaisser la béquille.
- *Réalisez des essais avec un autre doigt (par exemple index gauche), ou avec l'index droit différemment positionné sur le lecteur d'empreinte. Que constatez-vous ?*
  Pour un autre doigt : Il est impossible d'ouvrir la porte. La béquille tourne dans le vide.

  Pour l'index droit positionné différemment : Il est parfois impossible d'ouvrir la porte
- *Effacez un utilisateur de la mémoire et réessayez s'ouvrir la porte. Que constatez-vous ?* Il est de nouveau impossible de l'ouvrir avec ce code ou cette empreinte.
- *A partir des observations ci-dessus, que pouvez-vous dire sur la sécurité de la serrure ?* La sécurité de la serrure est bonne. Sans le code ou sans empreinte valide, impossible d'ouvrir la porte.
  Quelle(s) précaution(s) doit-on prendre lors de l'utilisation du lecteur d'empreinte ? Il faut faire attention à quel doigt poser et comment le poser pour l'empreinte.

2.Frontière d'étude

Le système étudié comprend :
- Le mécanisme de la serrure électronique (boîtier, partie électronique, béquilles, gâche, piles)

Ne sont pas inclus dans la frontière d'étude :
- La porte
- L'utilisateur

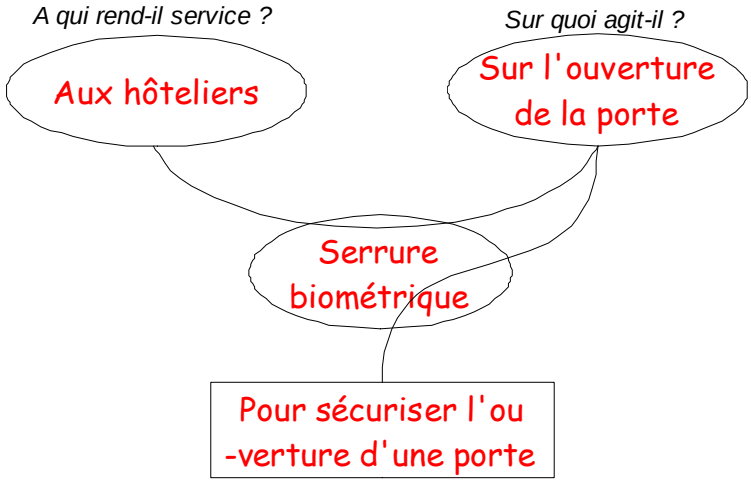
- *A partir des indications ci-dessus et du diaporama « Approche externe des systèmes », définissez la fonction globale du système étudié :* Autoriser ou interdire l'ouverture d'une porte.

- *Si le système étudié est maintenant constitué de la serrure électronique associée à la porte, que devient alors la fonction globale du système étudié ?* Autoriser ou interdire l'accès à un local.

3.Expression fonctionnelle du besoin

Afin d'identifier la clientèle type du fabriquant de cette serrure biométrique, consultez le document ressources « Clients.pdf ».

- *Quelle est la clientèle type du fabriquant de cette serrure biométrique ?*
  Il s'agit pour la plupart d'hôtels plutôt luxueux.
- *Complétez le graphe d'aide à l'expression fonctionnelle du besoin (diagramme « bête à cornes ») de la serrure biométrique ci-dessous :*

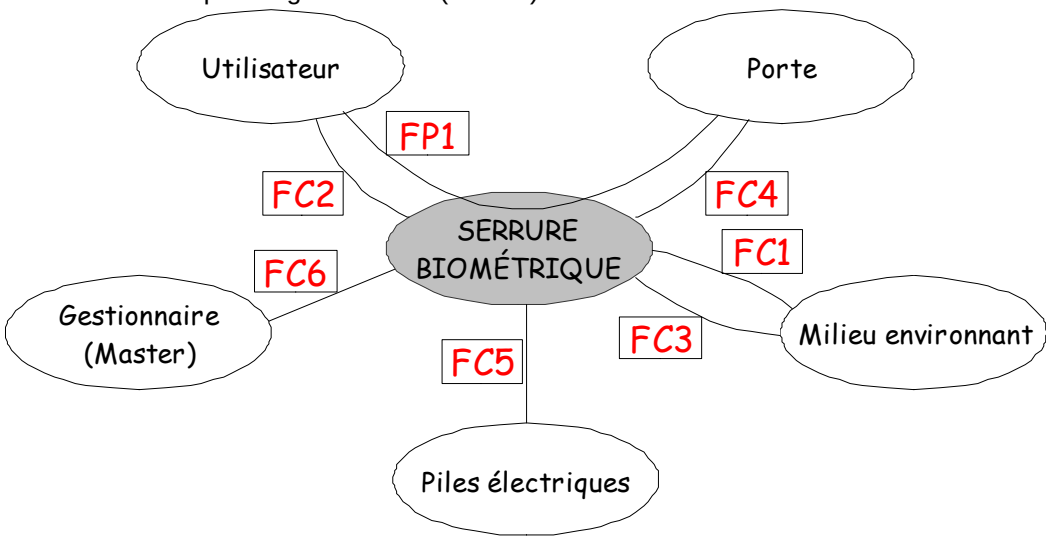


On rappelle que la frontière d'étude n'est constituée que de la serrure biométrique, sans la porte.

4.Graphe des interactions

- *On donne ci-dessous le graphe des interactions (diagramme pieuvre) ainsi que les fonctions de service correspondantes de la serrure biométrique. Replacez les fonctions de service sur le diagramme.*

FP1 : Autoriser ou interdire l'ouverture d'une porte par un utilisateur
FC1 : Résister aux agressions du milieu environnant
FC2 : Dialoguer avec l'utilisateur
FC3 : Ne pas polluer l'environnement
FC4 : S'intégrer à la porte
FC5 : Être alimenté en énergie
FC6 : Être administrable par un gestionnaire (Master)



5.Sécurité de la serrure

Présentation :

Notre serrure comporte plusieurs dispositifs d'ouverture, ce qui contribue à diminuer son niveau de sécurité.

En effet, plus il y a de dispositifs différents, plus il y a de possibilités, pour des personnes mal intentionnées, de les contourner.

Afin de prétendre à un éventuel label de certification de protection, il est indispensable d'évaluer chaque dispositif afin de déterminer sa résistance à l'intrusion.

Activités :

Il y a trois solutions pour autoriser l'ouverture de porte.

- *A partir du dossier technique et des manipulations précédentes, citez ces trois solutions :*
  Par empreinte
  Par code
  Par clé

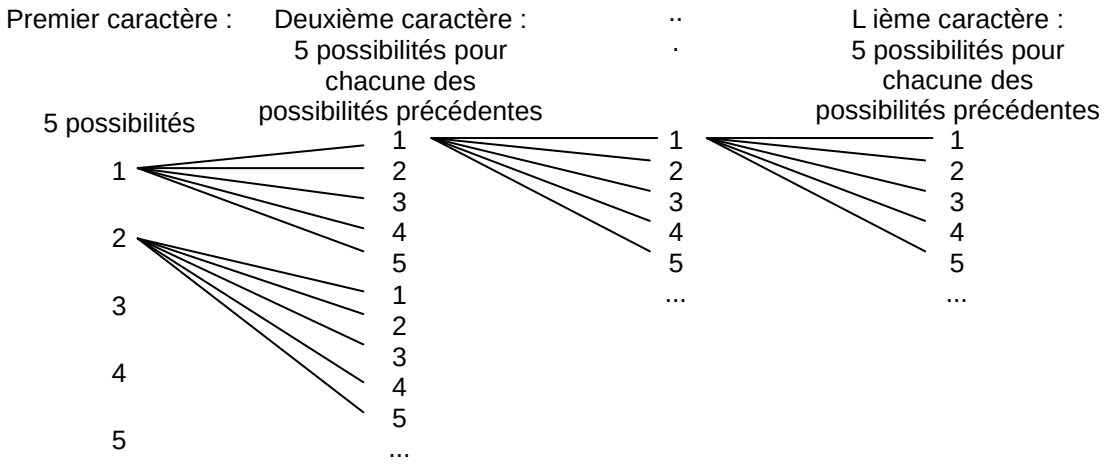
Le niveau de sécurité de la clé est ici difficilement évaluable. Les clés à goupilles (modèles à trous) utilisées ici existent dans des niveaux de qualité très différents : de la serrure très facilement ouvrable par « bumping », aux serrures d'une résistance exceptionnelle.

Le site http://protectvol.online.fr/cletrou.html donne des détails sur la sécurité de ce type de serrure.

Le code par clavier est une autre solution utilisable sur cette serrure.

- *Recherchez dans le dossier technique :*
  la longueur du code : L = 8 chiffres
  le nombre de caractères pouvant composer le code : n = n = 4 (de 0 à 3)

Le diagramme ci-dessous nous indique comment calculer le nombre de combinaisons possibles. L'exemple est donné pour un nombre de caractères n = 5 et une longueur du code L = 4



Le nombre de combinaisons différentes est ici 5 x 5 x 5 x 5 = n^L.

- *Calculez, pour la serrure étudiée, le nombre de combinaisons différentes :*
  On a 4 chiffres différents (n) et un code sur 8 caractères
  ce qui nous fait 4^8 = 65 536 combinaisons
- *Quelle est la probabilité, en saisissant un code au hasard, de tomber sur le master code ?*
  1 chance sur 65 536
- *Combien peut-on mémoriser de codes différents ?* 78 mots de passe différents

- *Quelle est alors la probabilité, en saisissant un code au hasard, de tomber sur un des codes mémorisés ?*
  P = 78 / 65536 = 1 / 840. On a une chance sur 840 de tomber sur un mot de passe valide.
- *Sur la serrure, chronométrez le temps mis pour saisir 5 codes non mémorisés (ouverture de la trappe, saisie d'un code à 8 chiffres, trois bips, fermeture de la trappe et ainsi de suite) :*
  On met environ 50 secondes, soit 10 secondes par tentative
- *En supposant que l'on tombe sur un bon code au bout de la tentative P (calculée deux questions avant), combien de temps une personne mal intentionnée met-elle pour trouver un code valide ?* Elle met 840 x 10 = 8400 secondes, soient 140 minutes (2h20) pour tomber sur un mot de passe valide.

Le label a2p signifie Assurance prévention protection ; il est délivré par l'Apsad (Assemblée plénière des sociétés d'assurances et de dommages) à la suite de tests permettant d'évaluer le temps de résistance de la serrure.

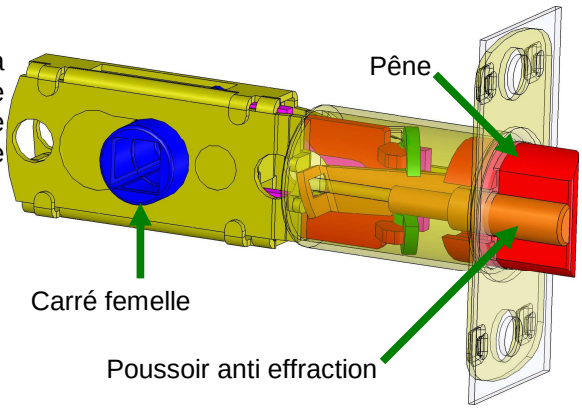
- Une serrure a2p * résiste 5 minutes.
- Une serrure a2p ** résiste 10 minutes.
- Une serrure a2p *** : 15 minutes.

- *Compte tenu des calculs précédents, notre serrure, du point de vue sécurité du code uniquement, pourrait-elle prétendre à un label A2P ?* On est largement au-dessus de ces valeurs. La serrure pourrait prétendre, de ce point de vue, à un label A2P.

On étudie maintenant le niveau de sécurité du système de lecture d'empreinte.

- *Relevez dans le dossier technique le taux d'acceptation d'empreintes fausses :* 0,0001%
- *En moyenne, combien de lectures d'empreintes faut-il réaliser pour obtenir l'acceptation d'une empreinte fausse ?* 1 / 0,0001 % = 1 million de lectures !
- *Mesurez le temps mis pour lire 5 empreintes fausses successives (ouverture de la trappe, lecture de l'empreinte, trois bips, fermeture de la trappe et ainsi de suite) :*
  Il faut environ 20 s pour lire 5 empreintes fausses (4 s par empreinte)
- *Combien de temps une personne mal intentionnée met-elle en moyenne pour obtenir l'acceptation d'une empreinte fausse ?* Il lui faudrait 4 millions de secondes, soit plus de 46 jours !
- *Compte tenu des calculs précédents, notre serrure, du point de vue sécurité du lecteur d'empreinte, pourrait-elle prétendre à un label A2P ?* On est largement au-dessus de ces valeurs. La serrure pourrait prétendre, de ce point de vue, à un label A2P.

La dernière étude de ce chapitre consiste à étudier la sécurité du pêne à l'effraction « à la carte de crédit ». Ce type d'effraction consiste à glisser une carte de crédit entre l'ouvrant et le dormant de la porte afin de repousser le pêne.



- *Porte ouverte, manipulez le pêne. Est-il possible de le repousser à la main ?* Oui
- *Fermez la porte en la claquant (sans abaisser la béquille) et observez le mouvement du pêne. Pour quelle raison le pêne doit-il pouvoir rentrer ?* Pour permettre le verrouillage de la porte lorsqu'on la referme en la claquant.

Lorsque la porte est fermée, le poussoir anti-effraction reste enfoncé alors que le pêne sort dans la gâche (partie creuse du dormant recevant le pêne), maintenant la porte fermée.

- *Maintenez enfoncé le poussoir anti effraction et appuyez sur le pêne. Peut-il se rétracter ?* Non
- *Le pêne est-il sécurisé contre l'effraction « à la carte de crédit » ?* Il est sécurisé contre ce type d'effraction.