Thème F Informatique embarquée et objets connectés

Chapitre 12 Objets connectés

Le thème F (*Informatique embarquée et objets connectés*) correspond aux deux chapitres suivants :

- Chapitre 11 : À la découverte de l'informatique embarquée
- **Chapitre 12 : Objets connectés**

Le chapitre 12 nécessite d'avoir traité le chapitre 11 au préalable.

A. Le programme

Les capacités exigibles du BO pour ce chapitre sont données ci-dessous. Les autres contenus du thème *Informatique embarquée et objets connectés* ont été traitées dans le chapitre 11.

Contenus	Capacités attendues du BO traitées dans le chapitre 12	Activités / Exercices
Commande d'un actionneur, acquisition des données d'un capteur	Écrire des programmes simples d'acquisition de données ou de commande d'un actionneur.	Activité 1 p. 172 Exercices 3 et 5 p. 178-179
Interface homme-machine (IHM)	Réaliser une IHM simple d'un objet connecté.	Activités 2 et 3 p. 173-175 Exercices 1, 2, 4 et 6 p. 178-179

B. QCM diagnostic p. 170

Ces questions vont instaurer le débat, ou la discussion.

Elles sont destinées à faire une évaluation diagnostic en début de chapitre et sont disponibles sur QCMCam et aux formats PDF, PPT et ODP sur le site web : https://lienbordas.fr/740171_ch12_qcm.

1	**Quel est l'avantage de la programmation par blocs pour une IHM simple ?** *Réponses :* **A.** Elle nécessite d'écrire du code complexe. **B.** Elle permet une programmation plus rapide et visuelle. (bonne réponse) **C.** Elle remplace tous les capteurs physiques. **D.** Elle empêche la création de boucles.
2	**En programmation par blocs, qu'appelle-t-on « événement » ?** *Réponses :* **A.** Une image **B.** Une commande pour allumer une LED **C.** Une action déclenchée par un clic ou un signal (bonne réponse) **D.** Une variable contenant un nombre
3	**À propos de la programmation par blocs, comme Scratch :** *Réponses :* **A.** il est impossible d'utiliser des variables à l'intérieur d'une boucle. **B.** il est impossible de programmer des boucles. **C.** il est possible de programmer des boucles. (bonne réponse)
4	**Quel type de bloc permet d'afficher une donnée lue depuis un capteur ?** *Réponses :* **A.** Le bloc « avancer de 10 pas » **B.** Le bloc « afficher texte » (bonne réponse) **C.** Le bloc « répéter indéfiniment » **D.** Le bloc « attendre 1 seconde »
5	**Pour qu'un robot muni de roues se déplace en ligne droite,** *Réponses :* **A.** il faut que ses roues aient des sens de rotation différents. **B.** il faut que ses roues aient des vitesses de rotation identiques. (bonne réponse) **C.** il faut que ses roues aient des vitesses de rotation différentes.

C. Frise historique p. 171

Réponses aux questions :

1. L'interface graphique joue le rôle d'intermédiaire entre l'homme et la machine. Souvent visuelle et fonctionnelle, elle permet de faciliter l'interaction, de rendre les commandes compréhensibles et d'offrir une expérience utilisateur intuitive.

2. L'utilisation de la souris permet une interaction fluide et directe avec la machine, simplement en bougeant la main ou en cliquant du bout des doigts. Cet outil rend la navigation plus intuitive, accélère l'exécution des tâches et améliore considérablement la productivité de l'utilisateur.

3. L'informatique ambiante (*Ambient Computing*) vise à effacer toute barrière physique entre l'homme et la machine, en supprimant les interfaces traditionnelles telles que le clavier ou la souris. Dans ce paradigme, l'utilisateur peut interagir de manière naturelle avec les systèmes numériques, par la voix, les gestes, ou même par la reconnaissance des émotions ou de la présence. L'objectif est de rendre la technologie invisible, omniprésente et parfaitement intégrée à l'environnement quotidien, pour une interaction fluide, intuitive et contextuelle.

D. Description des activités

Activité 1 p. 172 Comment programmer l'allumage des feux de détresse d'un véhicule ?

Capacité travaillée :

- Écrire des programmes simples d'acquisition de données ou de commande d'un actionneur.

Cette activité propose de simuler l'allumage des feux de détresse d'un véhicule à l'aide d'une carte micro:bit. Elle peut être réalisée avec ou sans matériel, en utilisant une carte réelle ou l'émulateur en ligne.

La programmation s'effectue par blocs, à la manière de Scratch. Le programme peut être téléversé sur une carte micro:bit, ou bien testé avec l'émulateur en ligne.

La programmation par blocs permet de faire le lien avec le travail mené au collège. Le programme ainsi écrit permet de programmer une interface homme-machine : par une pression sur les boutons A ou B, qui sont des capteurs d'entrée, les diodes peuvent clignoter ou s'éteindre (ce sont des actionneurs).

Réponses aux questions :

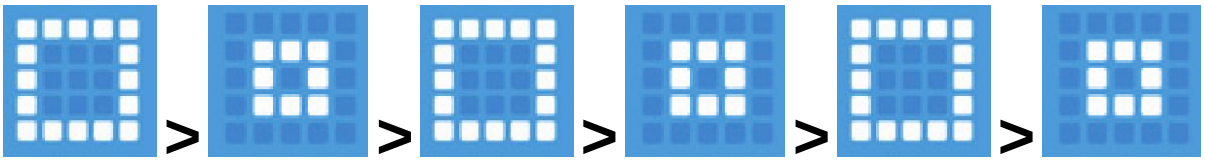
1. Les deux boutons A et B sont des capteurs : ils sont sensibles à un appui avec le doigt et peuvent être programmés indépendamment l'un de l'autre.

2. La carte micro:bit est dotée de 25 diodes, disposées selon un carré de 5 par 5. Chaque diode rouge peut être allumée ou éteinte de manière indépendante (par programmation) et son intensité lumineuse veut varier de 0 (éteinte) à 9 (allumée à fond). Sur l'image, 9 diodes sont représentées allumées.

3. Dans l'émulateur en ligne, on lance le programme en cliquant avec la souris sur le bouton « PLAY ». Au démarrage du programme, l'écran de la carte affiche une croix rouge.

4. Lorsque le bouton A est pressé, une variable nommée `warning` est initialisée et la valeur 1 lui est affectée. Cette information est déduite de l'examen du bloc « si » du programme (bloc de couleur verte).

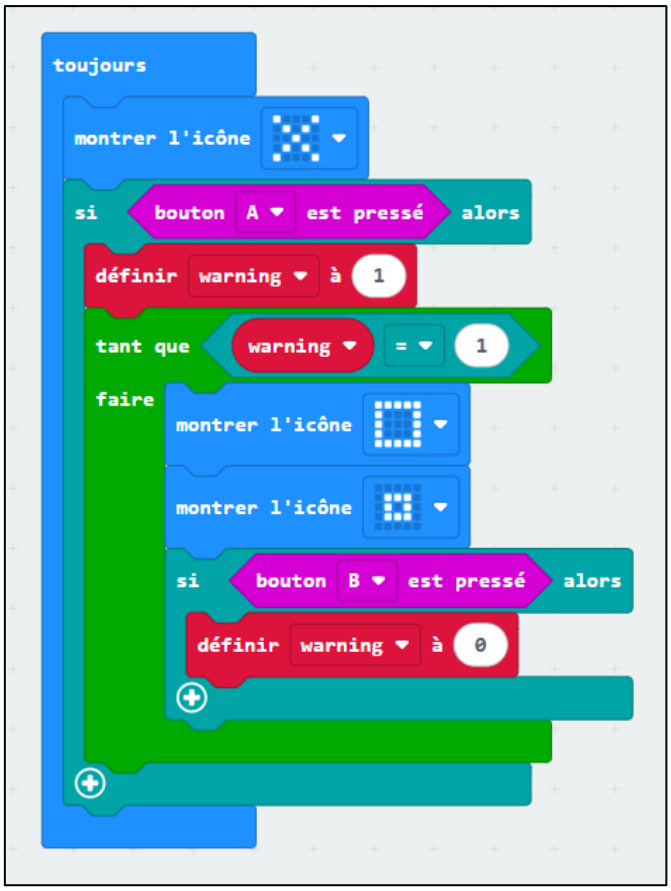
5. L'examen de la boucle « tant que » donne la réponse : tant que la variable `warning` contient la valeur 1, les deux icônes suivantes clignotent alternativement.



6. Pour éteindre les feux de détresse, il faut stopper la boucle « tant que », qui est une boucle infinie. Pour cela, il faut examiner la condition d'exécution de la boucle « tant que » qui est : « tant que la variable `warning` contient la valeur 1 ». Pour stopper la boucle « tant que » et arrêter le clignotement, il faut changer la valeur contenue dans la variable `warning`, en la passant à la valeur 0 par exemple (toute valeur est possible sauf la valeur 1).

Une possibilité est d'ajouter le bloc suivant **dans la boucle « tant que »**, afin que cette instruction soit évaluée à chaque tour de boucle :

On obtient le code suivant :



7. En changeant la valeur de la variable `warning`, on peut déclencher ou arrêter le clignotement des feux.

Le comportement programmé est le suivant :

« Si la variable `warning` contient la valeur 1, alors montrer les deux icônes alternativement. »
« Si la variable `warning` contient la valeur 0, alors ne rien faire. »

8. L'algorithme de comportement de cette interface est le suivant :

```
Algorithme feux de détresse
      Montrer l'icône X
      Si le bouton A est pressé :
            Définir une nouvelle variable nommée warning et lui affecter la
      valeur 1.
      Tant que warning est égale à 1 :
            Montrer l'icône « grand carré »
            Montrer l'icône « petit carré »
            Si le bouton B est pressé :
                  Affecter la valeur 0 à la variable warning
Fin algorithme
```

9. Le bouton activant les feux de détresse du véhicule doit être immédiatement accessible en cas d'urgence. Sa couleur rouge, universellement associée au danger, facilite son repérage rapide, même en situation de stress intense.

Activité 2 p. 173 Comment fonctionne une serrure connectée ?

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

Le but de cette activité est de comprendre le fonctionnement d'une serrure connectée, déverrouillable à distance depuis un smartphone utilisé comme télécommande.

Réponses aux questions :

1. Saisir le programme en blocs de la clé numérique dans l'émulateur en ligne à l'adresse makecode.microbit.org et le tester.

2.a. Quand on appuie sur le bouton A, le nombre 123 est envoyé par radio et l'écran de la carte micro:bit montre l'icône  .

b. Dans le cas d'une serrure connectée, la clé peut envoyer un signal à la serrure, afin de permettre son déverrouillage à distance. Deux types de signaux peuvent ainsi être envoyés par la clé à la serrure :

- signal de déverrouillage ;
- signal de verrouillage.

c. Le code 123 représente une information secrète transmise par la clé à la serrure, afin de déclencher son déverrouillage. Ce code doit rester strictement confidentiel afin que seul le détenteur de la clé puisse effectuer le déverrouillage de la serrure. Pour garantir cette sécurité, il est essentiel que le code soit chiffré lors de sa transmission (ce qui n'est pas le cas ici), afin d'éviter toute interception ou tentative de duplication frauduleuse.

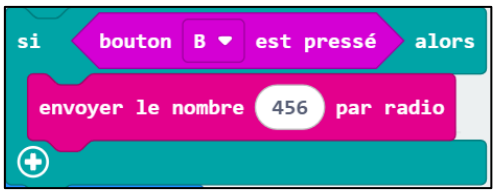
3. Saisir le programme en blocs de la serrure connectée et le tester.

4. a. L'affichage de l'icône  simule le déverrouillage de la serrure connectée.

b. Quand la serrure reçoit par radio le code 123, l'icône  s'affiche, qui simule le déverrouillage.

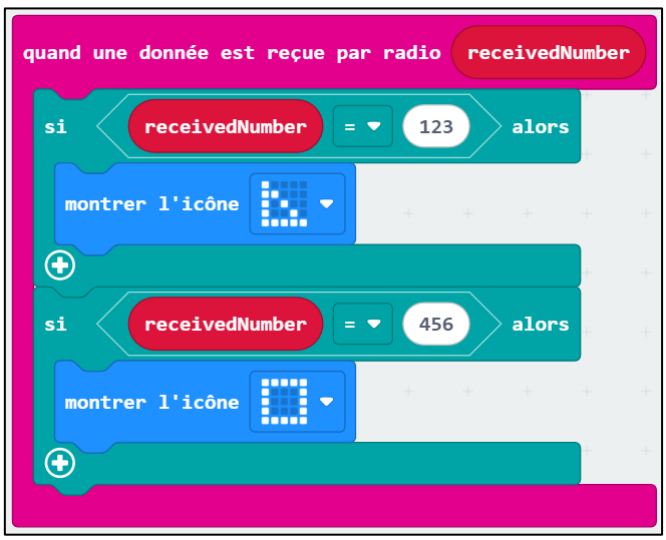
5. Il s'agit à présent de modifier le programme en blocs de la clé (et non pas celui de la serrure). Si le bouton B est pressé, alors le code 456 est envoyé par radio.

Le bloc à ajouter au code existant est le suivant :



6. Il s'agit à présent de modifier le programme en blocs de la serrure (et non pas celui de la clé). En effet, nous allons ajouter la fonctionnalité suivante : si la serrure reçoit le code 456, alors la serrure se verrouille, en affichant l'icône  .

Le code en blocs de la serrure devient alors :



7. L'intérêt d'une telle alerte est de renforcer la sécurité du système en informant immédiatement le propriétaire d'une activité potentiellement suspecte. Une tentative de déverrouillage ratée peut en effet indiquer qu'une personne non autorisée cherche à accéder au logement. Cette notification permet au propriétaire de réagir rapidement, par exemple en vérifiant les images d'une caméra de surveillance, en prévenant la police, ou en se rendant sur place. Elle contribue ainsi à dissuader les intrusions et à protéger les biens et les personnes.

8. Dans l'exemple de la clé et de la serrure, la conception d'une interface homme-machine (IHM) est nécessaire pour assurer une interaction claire, efficace et sécurisée entre l'utilisateur (l'homme) et le système de verrouillage (la machine).

Ici, l'homme est le propriétaire ou l'utilisateur légitime qui souhaite accéder à un espace sécurisé (comme un domicile ou un véhicule).

La machine, c'est la serrure connectée, qui contrôle l'accès en fonction des informations reçues (comme un code, une clé électronique ou une application mobile).

L'IHM peut prendre la forme d'un bouton, d'un lecteur de badge, d'un écran tactile ou d'une application mobile. Elle permet à l'utilisateur de transmettre une commande (par exemple, « ouvrir la porte ») et à la machine de fournir une réponse (par exemple, « accès autorisé » ou « accès refusé »). Une interface bien conçue garantit que cette interaction est intuitive, rapide, et sécurisée.

9. Une serrure connectée, qui peut être déverrouillée via un smartphone ou un badge RFID, ou encore commandée à distance via Internet, est un objet connecté. Elle appartient à l'Internet des objets (IoT) car elle peut :

- échanger des données (par exemple, envoyer une notification lors d'une tentative de déverrouillage) ;
- être contrôlée à distance (ouvrir/fermer via une application) ;
- interagir avec d'autres systèmes (comme une alarme ou une caméra de surveillance).

En conclusion, si la serrure intègre une connectivité (Bluetooth, Wi-Fi, etc.), elle peut être qualifiée d'objet connecté.

Activité 3 p. 174-175 Les objets connectés nous espionnent-ils ?

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

Capacité transversale travaillée :

- Développer une argumentation dans le cadre d'un débat et travailler l'oral.

L'objectif de cette activité sociétale est de sensibiliser les élèves aux enjeux que soulève l'usage des objets connectés collectant des données personnelles, en matière de sécurité et de liberté individuelle.

Réponses aux questions du parcours 1 :

1. Le Cyber Resilience Act est un règlement européen qui impose aux fabricants d'inclure dans leurs produits connectés : une configuration de sécurité par défaut, un système de mise à jour pour éviter les failles de sécurité, une protection contre les accès non autorisés via une authentification à deux facteurs (authentification qui demande deux confirmations d'identité différentes, par exemple un mot de passe puis un code envoyé par SMS), et une protection de confidentialité des données stockées (doc. B).

2. Il y avait 15,1 milliards d'objets connectés dans le monde en 2023 et les prévisions tablent sur 29,4 milliards pour 2030 (doc. D).

3. Les principales failles de sécurité des objets connectés peu élaborés concernent la collecte de données personnelles non indispensables à leur fonctionnement, ce qui peut permettre leur détournement ou leur prise de contrôle (doc. C). Leur faible niveau de sécurité génère des vulnérabilités techniques avec des mises à jour insuffisantes. Mais c'est également un manque d'information des utilisateurs qui les empêche de faire les bons choix ou de paramétrer correctement les objets connectés (doc. B).

4. Les objets connectés recueillent des informations sur leur environnement proche, ce qui peut porter atteinte à la vie privée des utilisateurs. Par exemple, si une personne malveillante réussit à s'introduire dans le système de vidéosurveillance d'une maison, elle peut regarder tout ce qui s'y passe. De même, en piratant un assistant vocal, on peut écouter les conversations privées dans un foyer (doc. A et C).

Éléments de réponse aux questions du parcours 2 :

Sont attendus les éléments suivants au cours du débat :

- bien comprendre qu'il s'agit ici d'un contexte fictif ;
- identifier les enjeux de société entre les gains en matière de sécurité apportés par les caméras de surveillance dans l'espace public et les reculs qu'implique ce type de dispositif en matière de liberté individuelle ;
- préciser ce qui est autorisé actuellement en France en matière de reconnaissance faciale : en 2025, les modes de surveillance avec reconnaissance faciale sont interdits, ou extrêmement contrôlés. Ces dispositifs techniques sont encadrés par le règlement européen sur l'intelligence artificielle qui limite très fortement leur usage ;
- en France, l'utilisation des données biométriques est interdite par la loi. Pendant les Jeux olympiques de Paris 2024, c'est une autre technique qui a été employée : les caméras dites « augmentées » ou « algorithmiques », permettant de détecter des mouvements de foule, des objets abandonnés ou encore des armes, mais pas d'identifier des personnes ;
- prolongement possible : donner des contre-exemples, comme celui de la surveillance généralisée en Chine.

E. Description des exercices

Exercice 1 p. 178 Gestion d'une lampe connectée

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

Cet exercice propose d'étudier l'interface homme-machine simple d'une lampe connectée, uniquement composée de boutons sur une télécommande.

1. Les boutons ON et OFF servent à allumer et à éteindre la lampe. Les boutons  servent à augmenter ou à diminuer la luminosité de la lampe. Les boutons colorés servent à sélectionner la couleur de la lampe.

2. Cette télécommande est équipée de boutons colorés qui permettent de modifier le comportement de la lampe d'une simple pression. Son utilisation paraît intuitive, ne nécessitant pas de mode d'emploi. L'interface homme-machine est donc lisible, accessible et adaptée à une utilisation immédiate par un être humain.

Exercice 2 p. 178 Écologie

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

L'objectif de cet exercice est d'étudier l'interface homme-machine d'une maison connectée. Grâce à un panneau de commande, il est possible de contrôler et de surveiller la consommation d'énergie de la maison.

1. Ce type de panneau de contrôle intelligent contribue à mieux respecter l'environnement de plusieurs façons par rapport aux systèmes traditionnels :

- contrôle centralisé des lumières : la possibilité d'éteindre toutes les lumières d'un seul geste évite les oublis et le gaspillage d'électricité, réduisant ainsi la consommation énergétique inutile ;
- gestion programmable du chauffage : en permettant de régler précisément la température et de définir des plages horaires, ce système évite le chauffage excessif ou inutile lorsque personne n'est présent, ce qui optimise la consommation d'énergie ;
- surveillance en temps réel de la consommation : l'affichage instantané de la consommation électrique sensibilise les utilisateurs à leur utilisation de l'énergie, les incitant à adopter des comportements plus responsables et à réduire leur empreinte écologique.

En combinant ces fonctionnalités, ce panneau de commande favorise une utilisation plus rationnelle et efficace des ressources énergétiques, contribuant ainsi à la protection de l'environnement.

2. Il est important de programmer des plages horaires pour le chauffage car cela permet d'ajuster la température en fonction des moments où le logement est occupé. Par exemple, on peut programmer le chauffage pour qu'il soit actif seulement le matin avant le réveil et le soir après le retour du travail, tout en le coupant durant la journée ou la nuit quand personne n'est à la maison. Cela évite de chauffer

inutilement, ce qui réduit la consommation d'énergie et les coûts associés. De plus, cela contribue à limiter l'impact environnemental en évitant le gaspillage d'énergie.

3. Avec l'évolution des technologies, la maison connectée pourrait intégrer de nouvelles fonctionnalités qui nécessiteraient une connexion à Internet pour offrir plus de confort et de sécurité. Parmi ces innovations, il est possible d'imaginer un système avancé de sécurité, basé sur la reconnaissance faciale et la surveillance à distance.

On pourrait ainsi envisager une maison connectée équipée d'un système de caméras avec reconnaissance faciale, qui identifie les personnes autorisées et envoie des alertes en temps réel au propriétaire en cas d'intrusion. Le propriétaire pourrait alors agir à distance grâce à la connexion Internet, améliorant ainsi la sécurité du logement et la réactivité en cas d'incidents.

4. Les interfaces homme-machine (IHM) jouent un rôle clé dans l'adoption de comportements écoresponsables chez les utilisateurs. Elles sensibilisent ces derniers à leur impact environnemental en fournissant des informations claires et facilement accessibles sur leur consommation énergétique. Par exemple, une IHM pourra afficher en temps réel la consommation d'électricité ou d'eau, incitant les usagers à limiter le gaspillage.

De plus, les IHM peuvent proposer des recommandations personnalisées, comme des alertes pour éteindre les appareils inutilisés ou optimiser le chauffage, encourageant ainsi des gestes écologiques simples. Elles rendent également les technologies plus intuitives, permettant à un plus grand nombre de personnes d'adopter facilement des solutions durables, comme la gestion automatisée de l'éclairage ou du chauffage.

Ainsi, les IHM contribuent à transformer les bonnes intentions en actions concrètes, en combinant information, simplicité d'utilisation et aide à la décision.

Exercice 3 p. 178 IHM d'un niveau à bulles

Capacité travaillée :

- Écrire des programmes simples d'acquisition de données ou de commande d'un actionneur.

Le but de cet exercice est de réaliser l'interface homme-machine d'un niveau à bulle à l'aide d'une programmation par blocs. Un niveau à bulle permet de vérifier l'horizontalité d'une surface.

1. L'instruction encadrée en noir indique qu'il est nécessaire d'effectuer la mesure de l'accélération de la carte (grâce au capteur d'accélération intégré) et d'affecter la valeur mesurée dans une variable nommée `lecture`.

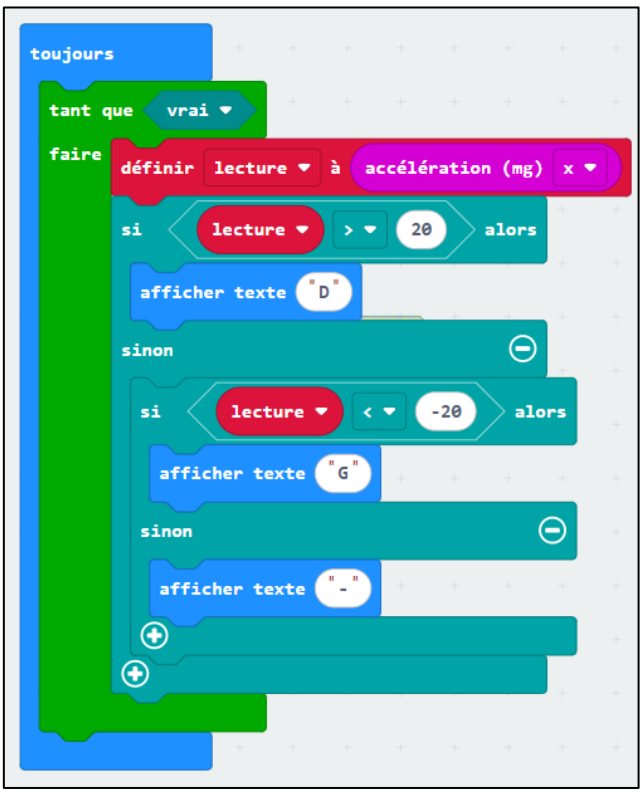
2. La boucle « tant que » est une boucle non bornée et la condition est toujours vraie, donc les instructions qui figurent à l'intérieur sont répétées à l'infini.

3. Il s'agit ici de compléter le programme en blocs pour modifier le comportement de la carte. Une des solutions possibles est d'ajouter un nouveau bloc « Si … Sinon » dans le premier bloc « Si ».

Le comportement du niveau à bulle ainsi programmé est le suivant :

- si le niveau est penché vers la gauche, alors il affiche « G » ;
- si le niveau est penché vers la droite, alors il affiche « D » ;
- sinon, il affiche « – », ce qui correspond à un niveau quasi horizontal.

On obtient le code suivant :



4. En fonction de son inclinaison, le niveau à bulle doit afficher « G », « D » ou « – ».

Exercice 4 p. 178 Gestion d'un thermostat connecté

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

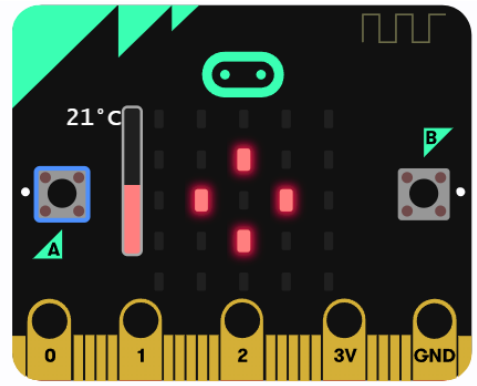
Cet exercice consiste à programmer une sonde de température qui mesure la température d'une pièce et envoie la valeur par radio à un thermostat.

1. Après un appui sur le bouton A, une boucle infinie (boucle « tant que ») est initialisée dans laquelle la valeur de la température de la pièce est envoyée par radio (après avoir été mesurée par un capteur de température) toutes les 1 000 millisecondes (1 s). De plus, une icône  est affichée à l'écran à chaque envoi de cette valeur.

2. Afin de pouvoir mesurer la température de la pièce, la sonde de température doit être munie d'un capteur de température.

3. Tous les 1 000 millisecondes, la valeur de la température est mesurée et envoyée par radio à la 2e carte.

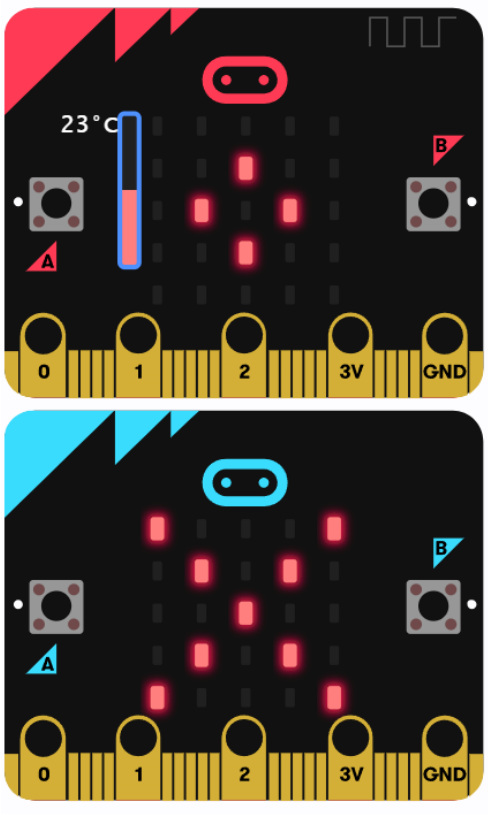
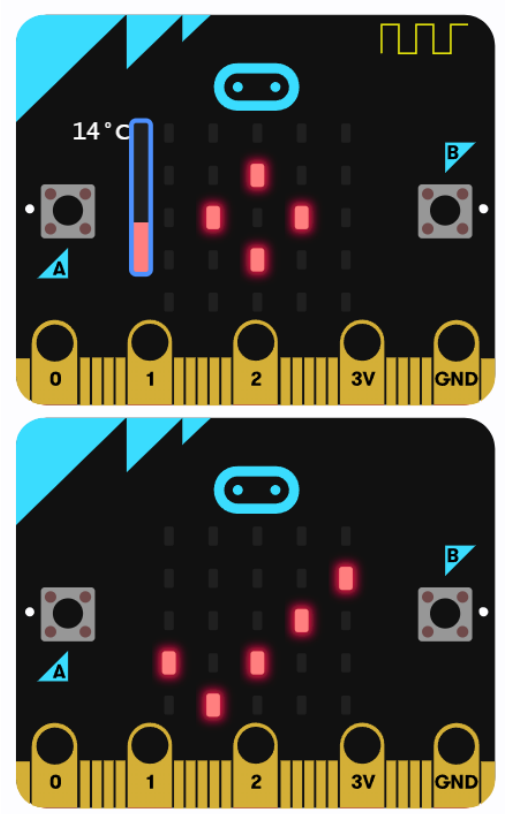
L’image suivante montre ce qui s’affiche :



4. Pour que la sonde envoie la valeur de la température toutes les 15 secondes, il faut remplacer 1000 par 5000, puisque 5 000 ms = 5 s.

5. Il s’agit à présent de compléter le code du thermostat qui doit recevoir la valeur envoyée par la sonde de température. En fonction de la valeur reçue, le thermostat doit afficher l’une des deux icônes suivantes :  ou  .

4. Une des solutions possibles est présentée page suivante.

Température inférieure à 18 °C (ici 23 °C) : le chauffage est éteint.	Température supérieure ou égale à 18 °C (ici 14 °C) : le chauffage est allumé.
	

Exercice 5 p. 179 Commande physique d'un robot

Capacité travaillée :

- Écrire des programmes simples d'acquisition de données ou de commande d'un actionneur.

Cet exercice consiste à faire avancer ou tourner un robot en lui transmettant une suite d'instructions, par l'intermédiaire d'une liaison série, par exemple. Les élèves sont ainsi amenés à comprendre qu'un ensemble de codes ou de règles permettent de donner des instructions au robot. Il s'agit là d'une ébauche de protocole de communication.

1. Le robot va avancer en ligne droite à 50 % de sa vitesse maximale pendant une seconde, puis tourner à gauche pendant une seconde, puis avancer pendant une seconde à 70 % de sa vitesse maximale, et enfin s'arrêter.

2. Pour que le robot effectue le mouvement demandé, il faut envoyer la séquence d'instructions suivante :

A75B75D5000A0B50D500A0B0.

Exercice 6 p. 179 Cybersécurité

Capacité travaillée :

- Réaliser une IHM simple d'un objet connecté.

L'objectif de cet exercice est d'étudier les éventuelles vulnérabilités d'une serrure connectée.

1. Une attaque par force brute consiste à tester systématiquement toutes les combinaisons possibles pour trouver une information secrète, comme un mot de passe, une clé de chiffrement, ou un code PIN.

2. Le chiffrement protège les données échangées contre les interceptions et les piratages. Sans chiffrement, un pirate peut lire, modifier ou rejouer les messages pour ouvrir la serrure. Avec chiffrement, les données sont illisibles sans la clé, ce qui garantit la sécurité de la communication.

3. Après trois codes erronés consécutifs, la serrure connectée devrait :

- verrouiller temporairement l'entrée de nouveaux codes (par exemple, 1 à 5 min) avec affichage d'un compte à rebours ;
- allonger progressivement le délai de blocage après chaque nouvelle série d'échecs ;
- notifier le propriétaire de la serrure (par push, e-mail ou SMS) de la tentative infructueuse ;
- déclencher une alarme locale (sonore et/ou visuelle) ou silencieuse ;
- consigner l'événement (date, heure, code masqué) dans un journal interne ou cloud ;
- exiger une authentification renforcée (code maître, biométrie) après plusieurs blocages ;
- réinitialiser le compteur d'erreurs après une période sans tentative (par exemple, 10 min).

Ces mécanismes combinés dissuadent d'une attaque par force brute, améliorent la détection d'intrusions et préservent l'expérience de l'utilisateur légitime.

4. Tenir un historique des tentatives de connexion permet de :

- détecter rapidement les attaques (par exemple, une attaque par force brute) ;
- analyser les incidents (traçabilité des accès) ;
- repérer les activités anormales (connexions à des horaires ou depuis des lieux inhabituels) ;
- prouver la conformité aux normes (RGPD, ISO 27001) ;
- renforcer en continu la sécurité (par des calculs statistiques et des ajustements).

F. Bilan du chapitre p. 180

Question	Réponse
1	**b. Une IHM**
2	**c. Une interface permettant à l'utilisateur de communiquer avec la machine**
3	**d. Éléments d'entrée, éléments de sortie et logiciel de contrôle**
4	**a. Une interface graphique**
5	**b. À répéter une action tant qu'une condition est vraie, comme actualiser l'affichage.**
6	**b. Elle définit des actions spécifiques à exécuter selon une condition donnée.**
7	**d. On paramètre deux machines pour qu'elles puissent communiquer entre elles.**
8	**b. La batterie de secours**
9	**c. Fournir une analyse en temps réel de l'environnement pour permettre des prises de décision rapides.**
10	**b. Temps réel**
11	**b. Parce que la sécurité est parfois négligée pour réduire les coûts.**
12	**a. S'assurer qu'elle fonctionne bien et réponde aux besoins des utilisateurs.**

Des QCM d'auto-évaluation sont disponibles pour un travail en autonomie de l'élève à l'adresse : https://lienbordas.fr/740171_ch12_bilan.