

Internet des objets connectés

Cours, exercices et cas pratiques

**Thierry Alhalel
Rémi Boule
Adrien van den Bossche**

DUNOD

© Dunod, 2023
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-086501-7

Sommaire

1	Notions sur le langage Python	1
1.1	Les structures de base en Python	2
1.1.1	Rappels de syntaxe	2
1.1.2	Structures conditionnelles	4
1.1.3	Listes	6
1.1.4	Dictionnaires	8
1.2	Fonctions en Python	9
1.3	Librairies usuelles	10
1.4	Librairies pour l'IoT	11
1.5	Exercices	13
2	Arduino et Langage C	25
2.1	Architecture générale des objets connectés	25
2.1.1	MCU et SoC	26
2.1.2	GPIO, capteurs et actionneurs	27
2.2	Manipulation d'une LED à travers les GPIO	29
2.2.1	LED simple	29
2.2.2	LED RGB	29
2.2.3	Exercices	30
2.3	Interaction avec des capteurs	34
2.3.1	Utiliser un capteur depuis un microprocesseur	34
2.3.2	Utilisation d'un capteur de luminosité (TSL2561)	36
2.3.3	Utilisation d'un capteur d'accélération (LSM303)	39
3	Notions sur les capteurs	43
3.1	Qu'est-ce qu'un capteur ?	43
3.2	Conditionnement et transmission	46
3.3	Jauges de contrainte	47
3.4	Les grands types de capteurs de température	49
3.4.1	Sonde à résistance de platine	50
3.4.2	Thermistance	50
3.4.3	Thermocouple	51
3.5	Capteurs basés sur l'effet piézoélectrique	52

3.6	Capteurs basés sur l'effet Hall	53
3.7	Capteurs basés sur l'effet photoélectrique	54
3.8	La conversion des données	56
3.9	Généralités sur le protocole I2C	58
3.10	Exercices	59
4	Acheminer les données	71
4.1	Récupérer de la donnée par HTTP	71
4.1.1	Format JSON	72
4.1.2	Désérialiser un JSON	73
4.2	Envoyer de la donnée par MQTT	74
4.2.1	Introduction rapide à MQTT	74
4.2.2	Utilisation dans l'environnement Arduino	76
4.3	Récupérer de la donnée par WebSocket	77
4.3.1	Protocole WebSocket	77
4.3.2	MQTT sur WebSocket	77
4.4	Envoyer de la donnée en LoRaWAN	79
4.4.1	Principes des réseaux LoRaWAN	79
4.4.2	Utilisation dans l'environnement Arduino	80
4.5	Exercices	80
4.5.1	HTTP	80
4.5.2	MQTT	82
4.5.3	WebSockets et JSON	85
4.5.4	LoRaWAN	86
5	Stocker les données	89
5.1	Bases relationnelles	90
5.1.1	Modèle conceptuel	90
5.1.2	Modèle logique	92
5.1.3	Requêtes SQL	93
5.1.4	Le modèle relationnel dans l'IoT	94
5.2	Base de données orientées séries temporelles	95
5.2.1	InfluxDB	96
5.2.2	TimescaleDB	98
5.3	Docker, Node-RED, InfluxDB, Grafana	100
5.3.1	Docker	100
5.3.2	docker-compose.yml	100
5.3.3	Node-Red	102
5.3.4	Formater pour influxDB	103
5.3.5	Grafana	103
5.4	Exercices	104
5.4.1	Docker et NodeRED-UI	104
5.4.2	TimescaleDB	107

6	Analyse des données	109
6.1	Statistiques élémentaires	110
6.1.1	Série statistique à une variable	110
6.1.2	Série statistique à deux variables	111
6.2	Évaluation des incertitudes de mesures	112
6.2.1	Présentation d'un résultat expérimental	112
6.2.2	La propagation des incertitudes	113
6.2.3	Les différentes incertitudes	114
6.2.4	Un peu plus sur les intervalles de confiance	117
6.3	Ajustement de données	118
6.3.1	Régression linéaire : méthode des moindres carrés	119
6.3.2	Régression linéaire : la covariance	120
6.3.3	Incertitudes sur A et B	120
6.3.4	Ajustement exponentiel de données	121
6.3.5	Ajustement quadratique de données	121
6.4	Le test du χ^2	121
6.4.1	Principe	121
6.4.2	Hypothèse nulle et p-valeur	122
6.5	Exercices	123
6.5.1	Séries statistiques	123
6.5.2	Calcul des incertitudes de mesures	131
6.5.3	Ajustements linéaires et non linéaires	135
6.5.4	Test du χ^2	138
6.6	Quelques éléments sur l'analyse en composantes principales	143
6.6.1	Des éléments clés	143
6.6.2	Un exemple d'ACP avec RStudio	144
6.7	Les tables	149
7	Cryptographie et sécurité	153
7.1	Cryptographie classique	155
7.1.1	César	156
7.1.2	Vigenère	157
7.1.3	Quel bilan ?	158
7.2	Cryptographie symétrique	159
7.2.1	AES	159
7.2.2	S-box AES	163
7.2.3	Chiffrement	165
7.2.4	Déchiffrement	165
7.2.5	Modes de chiffrement	165
7.3	Cryptographie asymétrique	168
7.3.1	Forces et faiblesses de la cryptographie symétrique	168
7.3.2	Comment s'échanger une clé ?	168
7.3.3	Cryptographie à clé publique	170
7.3.4	RSA	170
7.4	Le hachage	174

7.4.1	Fonction de hachage cryptographique	174
7.5	AES dans l'IoT avec LoRaWAN	175
7.5.1	LoRaWAN	175
7.5.2	Activation de l'objet	176
7.5.3	Clés de session	176
7.5.4	Analyse d'un paquet de données	177
7.5.5	Accès à la donnée	178
7.5.6	Chiffrement en LoRaWAN	179
7.6	Futur de la cryptographie pour l'IoT	181
7.6.1	ASCON	181
7.7	Exercices	182
7.7.1	Chiffrement de César	182
7.7.2	Attaques sur le chiffrement de César	183
7.7.3	Chiffrement de Vigenère	184
7.7.4	Attaque sur le chiffrement de Vigenère	185
7.7.5	Arithmétique modulaire	187
7.7.6	Division de polynômes	187
7.7.7	Fondements mathématiques d'AES	188
7.7.8	Structure d'un paquet LoRaWAN	189
7.7.9	Cryptographie en LoRaWAN	191
8	Exercice de synthèse	195
8.1	Conception du système général	197
8.1.1	Objectifs et architecture générale	197
8.1.2	Introduction à la conception	197
8.2	Étude de la pince ampèremétrique	198
8.2.1	Découverte de la pince	198
8.2.2	Expérimentation	200
8.3	Interfaçage avec le microcontrôleur	203
8.3.1	Prise en main et vérification de l'Arduino	203
8.3.2	Microcontrôleur et ADC	204
8.3.3	Mise en œuvre du Controllino	204
8.4	Transmission des données	210
8.4.1	Description du format d'un échantillon de mesure	211
8.4.2	Transport de la donnée avec MQTT	211
8.4.3	Contrôle de la remontée des échantillons	216
8.5	Enregistrement des données en base	218
8.5.1	Récupération des données et mise en base	218
8.5.2	Génération d'un message MQTT de test	220
8.5.3	Création de la base de données	220
8.5.4	Vérification des données enregistrées en base	221
8.6	Exploitation des données dans un <i>dashboard</i>	222
8.6.1	Création d'un premier <i>dashboard</i> simple	222
8.6.2	Plusieurs pinces dans le même <i>dashboard</i>	223
8.6.3	Jauge, dernière valeur et répétition par capteur	224

1

Notions sur le langage Python

Python est un langage de programmation interprété très utilisé dans le domaine de l'Internet des Objets. Il permet de traiter facilement de grands volumes de données venant de capteurs par exemple, de les représenter graphiquement, de les stocker en bases de données, etc. L'objectif de ce chapitre est de rappeler quelques notions de base concernant ce langage mais aussi de découvrir les principales librairies que vous allez utiliser dans vos projets IoT (Internet of Things, Internet des objets en anglais).

Sommaire

1.1	Les structures de base en Python	2
1.1.1	Rappels de syntaxe	2
1.1.2	Structures conditionnelles	4
1.1.3	Listes	6
1.1.4	Dictionnaires	8
1.2	Fonctions en Python	9
1.3	Librairies usuelles	10
1.4	Librairies pour l'IoT	11
1.5	Exercices	13

Il est entendu qu'il ne s'agit nullement de décrire ici le langage Python de manière exhaustive, mais bien de faire un résumé des notions nécessaires à l'objectif du chapitre.

Comme vous avez déjà étudié les rudiments du langage Python, vous savez que c'est un langage interprété (non compilé), orienté objet et sous licence libre. Ce langage est utilisé sous tous les principaux systèmes d'exploitation : Windows, GNU/Linux, Unix, Android et macOS.

Dans cet ouvrage, nous utiliserons la version Python 3. Il existe plusieurs façons d'écrire et de tester du code en Python. Vous pouvez bien sûr conser-

ver celle que vous avez apprise lors de vos études, mais sachez que les codes présentés ici sont testés :

- en environnement Linux avec l'éditeur Scite qui permet de développer et de tester du code Python de façon minimaliste ;
- en environnement Windows 7/10 ou Linux avec le logiciel Spyder 3 ;
- en environnement Anaconda, qui est une distribution libre open source de Python et R, installable sur les OS Windows et Linux, et permettant de traiter des données en quantité. Anaconda se présente comme un navigateur donnant accès en particulier à Spyder, Jupyter Notebook et RStudio.

L'une des principales forces de Python est l'existence de nombreuses librairies qui donnent accès à de puissantes possibilités graphiques et de calculs numériques.

Dans cet ouvrage, nous vous présenterons des programmes complets et fonctionnels soit dans les rappels de cours (la première ligne portera l'indication code *a.b*) soit dans les exercices (la première ligne comportera alors la mention exercice *a.b*). L'entier *a* renvoie au numéro de chapitre (ici le premier) et le second entier, *b*, indique le numéro de code au sein du chapitre. Vous pourrez utiliser cette nomenclature pour retrouver le code à télécharger sur le site de Dunod.

1.1 Les structures de base en Python

Nous ne ferons pas ici un cours de programmation, mais nous insisterons sur les notions essentielles du langage Python et de ses librairies.

1.1.1 Rappels de syntaxe

Le langage **Python** est naturellement **indenté** pour les blocs de code : boucles, sous-routines, tests conditionnels... vous devez absolument y faire attention. Voici un exemple de code fonctionnel avec indentation (tout ce qui est dans l'indentation fait partie du bloc d'instructions de la boucle) :

```
1  # code 1.1
2  # appel librairies
3  import random
4  import math
5  # initialisation des constantes et listes
6  N=1000;
7  DEDANS=0;
8  xdedans=[];
9  ydedans=[];
10 xdehors=[];
11 ydehors=[];
12 # boucle principale
```



```
13 for i in range(N):
14     a, b = random.uniform(-1.,1.), random.uniform(-1.,1.)
15     longueur = math.sqrt(a**2 + b**2)
16     if longueur < 1:
17         xdedans.append(a)
18         ydedans.append(b)
19     DEDANS=DEDANS+1
20     else:
21         xdehors.append(a)
22         ydehors.append(b)
23 print(DEDANS)
```

On note dans le code qui précède, les indentations successives de la boucle `for` et de la condition `if`, car la conditionnelle (indentée) fait partie intégrante de la boucle (indentée). Autrement dit, **l'augmentation de l'indentation** signe le démarrage d'un nouveau bloc d'instructions.

Le code se structure de la façon suivante :

1. l'importation des librairies (ici la librairie `random` qui contient les lois de probabilités (la loi uniforme pour nous) et la librairie `math` qui contient les fonctions mathématiques classiques (racine carrée (`sqrt`) pour nous));
2. la déclaration des constantes et l'initialisation des tableaux (il y en a quatre, lesquels?);
3. le cœur du programme, avec le calcul de l'entier `DEDANS` qui est forcément inférieur ou égal à `N` (pourquoi?);
4. le code permet également de remplir (instruction `append`) les quatre listes avec les valeurs de `a` et `b` qui répondent à la condition imposée par le `if`,
5. l'affichage final du résultat `DEDANS` (remarquons la position de cet affichage par rapport à la boucle `for`).

Les **commentaires** (sur une ligne) sont réalisés à l'aide du caractère dièse : `#`. Il est important d'en mettre dans un code de façon à le rendre clair et compréhensible.

Dans le langage Python les variables sont typées **dynamiquement**, c'est-à-dire que le type d'une variable peut changer en cours d'exécution, comme sur le code ci-dessous :

```
1 # a est entier
2 a= 1
3 print('a est entier : ',a)
4 # a devient flottant
5 a=a*1.0
6 print('a devient flottant :', a)
```

avec le résultat suivant (on passe d'un entier à un type flottant) :

```
1 ('a est entier : ', 1)
2 ('a devient flottant :', 1.0)
```

1.1.2 Structures conditionnelles

La **structure conditionnelle** `if` se définit en Python :

```
1 if condition1:
2     instructions1
3 else:
4     instructions2
```

le `else` n'est pas obligatoire. Noter l'indentation utilisée.

On réalise une **répétition conditionnelle** en Python avec la boucle `while`.

```
1 while condition:
2     instructions
```

Tant que la condition est vraie, la boucle `while` continue, et si le programme est mal conçu on peut tomber dans le piège de la **boucle infinie**, le programme ne peut alors pas se terminer. Pour illustrer le principe de la boucle `while`, on peut mettre en place l'**algorithme d'Euclide**, qui permet de trouver le **PGCD** (plus grand diviseur commun) de deux entiers strictement positifs a et b ($a \geq b$) :



Algorithme d'Euclide

- On affecte à la variable entière x la valeur entière a
- On affecte à la variable entière y la valeur entière b
- On affecte au compteur entier i la valeur 0

Tant que y est différent de 0 : (boucle `while`)

1. On incrémente le compteur i de 1 unité
2. On calcule le reste r_i de la division entière de x par y
3. On affecte à la variable x la valeur de y
4. On affecte à la variable y la valeur de r_i

À la sortie de la boucle `while` au bout de n itérations, le **PGCD(a,b)** est la dernière valeur de x (ou de y ce qui revient au même).

Par exemple si $a = 455$ et $b = 84$, le PGCD de ces deux entiers vaut 7 : on va représenter les étapes successives de l'algorithme qui mènent au résultat à l'aide d'un tableau qui représente ce qui se passe dans la boucle `while` (attention, c'est avant la boucle que x prend la valeur 455 et y la valeur 84) :

itération i	variable x	variable y	reste r_i
1	84	35	35
2	35	14	14
3	14	7	7
4	7	0	0

Voici la conclusion du programme : le PGCD de 455 et 84 est donc de 7. Le code Python correspondant pour la détermination du PGCD de deux entiers est :

```
1 # code1.2
2 # Entiers a et b dont on cherche le PGCD
3 a = 306
4 b = 756
5 # Test avec assert : les nombres sont bien positifs et a > b
6 assert (a > 0) and (b > 0)
7 if a < b:
8     a, b = b, a # Intversion si besoin : on impose que a >= b
9
10
11 a0, b0 = a, b # On garde une copie des valeurs originales
12 # On boucle (while) jusqu'a ce que le reste soit nul
13 while b != 0:
14     a, b = b, a % b
15 # On remplace a par b et b par le reste de la division euclidienne de a par b
16
17 print('Le PGCD de {} et {} vaut : {}'.format(a0, b0, a) # On affiche le
    resultat
```

En voici le résultat :

```
1 Le PGCD de 756 et 306 vaut : 18
```

On réalise une **répétition inconditionnelle** (de N itérations) en Python avec la boucle **for** :

```
1 for i in range(1,N+1):
2     instructions
```

Ici N est un entier, et i le compteur. Il est important de noter que l'entier i va varier de la valeur initiale 1 jusqu'à N .

Prenons comme exemple d'application la **fonction factorielle** d'un entier naturel n :

On définit en mathématiques la fonction factorielle d'un entier $n \geq 0$ (notée $n!$) comme :

$$\text{factorielle}(n) = n! = 1 \times 2 \times 3 \times \cdots \times (n-1) \times n$$

avec par convention :

$$0! = 1! = 1$$

et par exemple :

$$6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 = 720$$

et

$$7! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 = 5040$$