CORRIGÉ NON OFFICIEL

BTS Cybersécurité, Informatique et réseaux, Électronique

E4 - Étude et conception de réseaux informatiques

Session 2026

Proposition de corrigé rédigée par FormaV pour s'entraîner. Ce n'est pas le corrigé officiel de l'examen et elle ne remplace pas les éléments de correction officiels.

Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour consulter tous nos sujets d'annales et corrigés du BTS CIEL, veuillez visiter :
coursbtsciel.fr/annales-sujets-et-corriges

BREVET DE TECHNICIEN SUPÉRIEUR CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

Option A – Informatique et Réseaux

Épreuve E4 – Étude et conception de réseaux informatiques – Session 2026

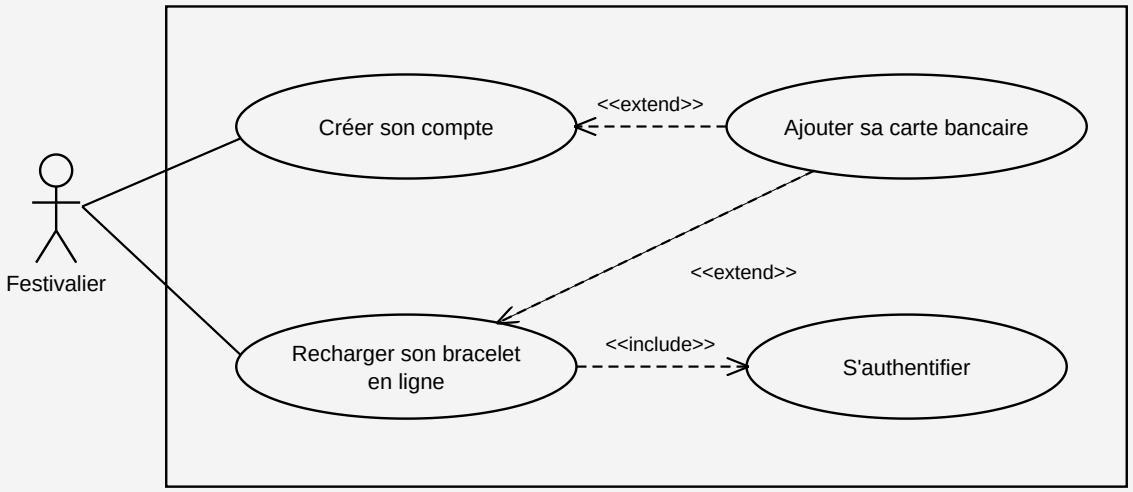
PROPOSITION DE CORRIGÉ

Proposition de corrigé établie par FormaV à partir du sujet, non officielle. Elle ne préjuge pas des consignes nationales de correction données aux jurys.

PARTIE 1 – ANALYSE DU SYSTÈME INFORMATIQUE

Question 1

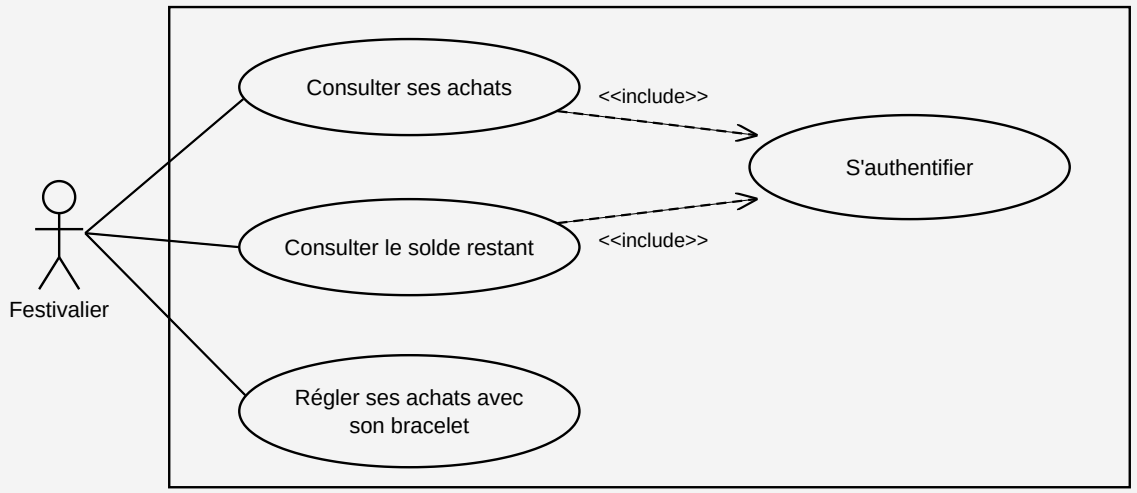
- « Ajouter sa carte bancaire » étend « Créer son compte » (relation <<*extend*>>, flèche pointillée de « Ajouter sa carte bancaire » vers « Créer son compte ») : l'ajout de la carte est facultatif (« Bien que ce ne soit pas obligatoire »).
- « Recharger son bracelet en ligne » inclut « S'authentifier » (relation <<*include*>>, flèche pointillée de « Recharger son bracelet en ligne » vers « S'authentifier ») : le rechargement en ligne passe systématiquement par l'authentification.
- « Ajouter sa carte bancaire » étend « Recharger son bracelet en ligne » (relation <<*extend*>>, flèche pointillée de « Ajouter sa carte bancaire » vers « Recharger son bracelet en ligne ») : la carte n'est saisie au moment du rechargement que si aucune carte n'a été enregistrée à la création du compte.
- Aucune relation entre « Créer son compte » et « S'authentifier ».



DR-Pro1 complété : relations entre les cas d'utilisation

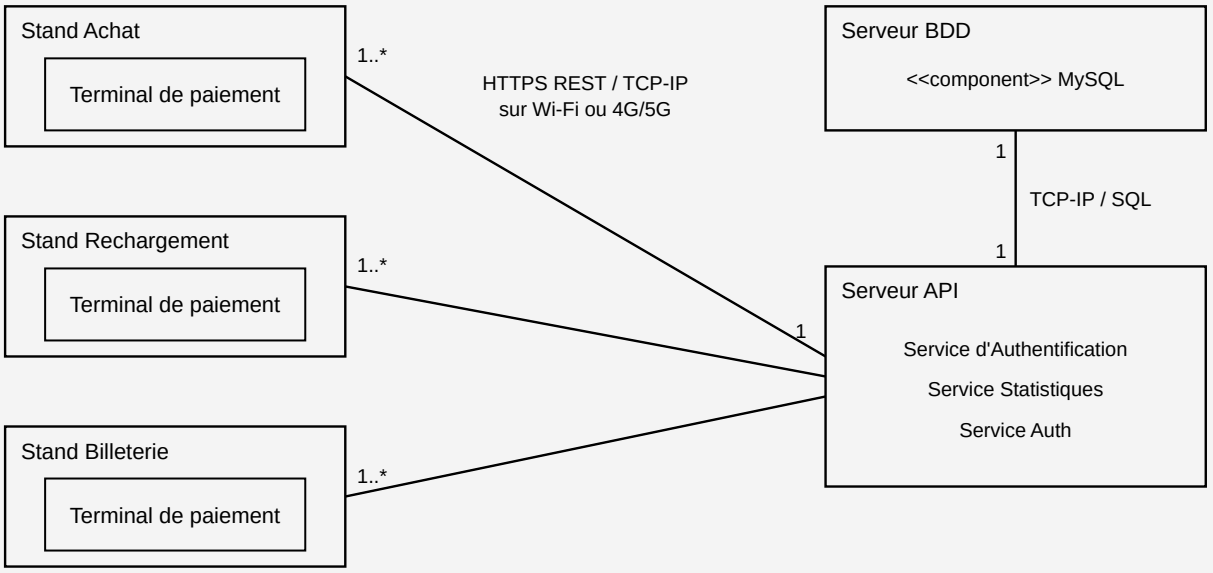
Question 2

Les cas « Consulter ses achats » et « Consulter le solde restant » sont rattachés à l'acteur festivalier par une association simple. Chacun est relié au cas « S'authentifier » par une relation <<*include*>> (flèche pointillée du cas de consultation vers « S'authentifier »), car la consultation n'est possible qu'après authentification. Aucune relation n'est nécessaire avec « Régler ses achats avec son bracelet ».



DR-Pro2 complété : ajout des cas de consultation

Question 3



DR-Pro3 complété : liaisons entre les nœuds

Nœud A	**Nœud B**	**Support / protocole**	**Cardinalités**
Chaque stand (Achat, Rechargement, Billeterie) : Terminal de paiement	Serveur API	HTTPS REST / TCP-IP sur Wi-Fi ou 4G/5G	1..* terminaux pour 1 Serveur API
Serveur API	Serveur BDD (MySQL)	TCP-IP / SQL	1 pour 1

Les supports sont ceux de la figure 6 (« HTTPS REST / Wi-Fi / 5G » pour le terminal, « TCP-IP / SQL » entre les API et le SGBDR).

Question 4

Support	Avantages entourés	Inconvénients entourés
Téléphone portable (écran 4 pouces, terminal Cashless)	Mobilité ; Connexion 4G/5G	Taille de l'écran ; Recharge de la batterie
Tablette (écran 10 pouces, Wi-Fi)	Mobilité ; Taille de l'écran	Recharge de la batterie
Ordinateur portable (écran 17 pouces, Wi-Fi)	Taille de l'écran ; Mobilité	Recharge de la batterie
Ordinateur fixe (écran 24 pouces)	Taille de l'écran	Difficile à déplacer

Question 5

Couche physique	OUI / NON
Wi-Fi	OUI
Ethernet	OUI
I2C	NON
4G / 5G	OUI

Le Wi-Fi et la 4G/5G sont les deux accès sans fil des terminaux (figure 8). Ethernet relie le réseau festival à l'infrastructure. L'I2C est un bus interne de composants, non utilisé entre terminal et serveur.

Question 6

Protocole	OUI / NON	Nom de la couche (OSI)
HTTPS	OUI	Application (couche 7)
IP	OUI	Réseau (couche 3)
SSH	NON	Application (couche 7)
UDP	NON	Transport (couche 4)

HTTPS (HTTP REST chiffré par TLS) et IP sont nécessaires à l'échange entre le terminal et le serveur d'APIs. SSH n'est pas un protocole de l'échange applicatif. UDP n'est pas utilisé, les échanges reposant sur TCP.

Question 7

Oui, un utilisateur peut avoir plusieurs bracelets. Dans la table bracelets, la clé étrangère user_id référence la table users, sans contrainte d'unicité sur cette colonne. La relation users–bracelets est donc de type 1 à plusieurs (1,n) : un festivalier peut être associé à plusieurs bracelets, par exemple sur des évènements différents, chaque bracelet étant lié à un évènement (event_id).

Question 8

Création de la table stands, à partir du schéma de la figure 9 et de la syntaxe de la documentation DT1 :

```
CREATE TABLE stands (
    id INT PRIMARY KEY AUTO_INCREMENT,
    event_id INT,
    label VARCHAR(100),
    kind VARCHAR(50),
    is_autonomous BOOL,
    FOREIGN KEY (event_id) REFERENCES events(id)
);
```

Question 9

```
SELECT terminals.ip_address
FROM terminals JOIN stands
ON terminals.stand_id = stands.id
WHERE stands.is_autonomous = TRUE;
```

Question 10

Le contrôleur WLC3504 est retenu car il répond aux exigences du cahier des charges (DT2) :

- Gestion centralisée : il assure « un contrôle, une gestion et un dépannage centralisés » des réseaux sans fil, et permet la configuration groupée des points d'accès.
- Bande 5 GHz : la fonction band steering dirige automatiquement les clients vers la bande 5 GHz.
- Répartition des connexions : la fonction load balancing équilibre la charge des clients entre les points d'accès.
- Sécurité renforcée : il supporte WPA3 pour le chiffrement et 802.1X pour l'authentification des utilisateurs, avec une détection des intrusions.
- Capacité : 150 points d'accès et 3000 clients, largement suffisants pour le festival (deux AP, sept stands de distribution et deux stands de recharge).

Question 11

Les trames de la figure 10 correspondent à un échange TLS 1.3 en reprise de session par PSK :

- Trame 4 (Client Hello, figure 11) : l'extension pre_shared_key (len=331) est présente, ce qui signale une reprise par PSK. Elle est accompagnée d'une extension key_share (x25519), exigée par DT3 pour permettre au serveur de revenir à une négociation complète, ainsi que de supported_versions (TLS 1.3, TLS 1.2).
- Trame 6 (Server Hello, figure 12) : le serveur répond avec une extension pre_shared_key (len=2) pour accepter la reprise et une extension key_share (x25519) pour l'échange de clé (EC)DHE. L'extension supported_versions (len=2) du Server Hello vaut TLS 1.3 : c'est la version effectivement négociée, le champ Version à TLS 1.2 (0x0303) n'étant conservé que pour la compatibilité. La suite TLS_AES_256_GCM_SHA384 (0x1302) est une suite propre à TLS 1.3 (DT3).

- Même Session ID (7749b3bd…852a) dans le Client Hello et le Server Hello, et pre_shared_key acceptée par le serveur : d'après DT3, le serveur s'authentifie alors par la clé PSK, sans envoyer de certificat ni de message CertificateVerify. La trame 6 enchaîne Server Hello, Change Cipher Spec et Application Data sans message Certificate ni CertificateVerify, ce qui est conforme à la reprise PSK décrite par DT3.
- Les trames suivantes (Change Cipher Spec, Application Data) confirment l'établissement d'un canal chiffré.

Ces éléments démontrent un échange TLS 1.3 avec reprise PSK.

Question 12

- Suite de chiffrement (trame 6, « Cipher Suite ») : TLS_AES_256_GCM_SHA384 (0x1302).
- Chiffrement symétrique : AES en mode GCM, clé de 256 bits.
- Fonction de hachage : SHA-384.

Question 13

Le hachage transforme un message de taille quelconque en une empreinte de taille fixe. Cette transformation est à sens unique : on ne peut pas retrouver le message à partir de l'empreinte, et il n'existe pas de clé de déchiffrement. Il sert à vérifier l'intégrité des données.

Le chiffrement transforme un message en un message illisible à l'aide d'une clé, et il est réversible : le déchiffrement permet de retrouver le message original avec la clé appropriée. Il assure la confidentialité des échanges.

Question 14

Le nom de domaine du site est ciss.fr (chemin : /cashlessonline/tpe/init/).

Question 15

Une API REST utilise les méthodes HTTP GET (lecture), POST (création), PUT ou PATCH (mise à jour) et DELETE (suppression), qui correspondent aux opérations CRUD (Create, Read, Update, Delete).

Question 16

Le body de la requête contient notamment le numéro de stand « Stand » : 8, la licence « License » : « 542 », la ligne « Row » : « 001 » et le numéro de série « SerialNumber ».

Question 17

Le body indique "Stand": 8. D'après la légende de la figure 5, le stand 8 est le point de vente Snack 4.

Question 18

SerialNumber est le numéro de série unique du terminal (identifiant de type UUID, ici 9dbca32c-b3f2-4844-9372-39069f3acfcc). Il permet d'identifier de manière unique le terminal auprès du serveur d'APIs.

Question 19

Le code 200 est le code d'état HTTP « OK » : il indique que la requête a été reçue, comprise et traitée avec succès par le serveur.

Question 20

La valeur APIKey est une clé d'API attribuée au terminal lors de son initialisation. Elle identifie et authentifie le terminal pour les requêtes suivantes adressées au serveur.

Question 21

Un timestamp (horodatage) est une valeur numérique qui représente un instant précis, généralement le nombre de millisecondes écoulées depuis le 1er janvier 1970 à 0 h UTC (époque Unix). Il sert ici à dater la requête et à rendre l'URL unique.

Question 22

Une session sur un serveur web permet de conserver un état entre plusieurs requêtes, alors que le protocole HTTP est sans état. Le token de session identifie le client et lui évite de se réauthentifier à chaque requête.

Question 23

Les tables utilisées pour générer la réponse de l'échange 3 sont : terminals (identification du terminal par terminal_uid et affectation à un stand par stand_id), stands (libellé du stand, label) et events (nom de l'évènement, name, repris dans AddressLine1, et lieu, location).

Question 24

```
INSERT INTO events (name, date_start, date_end, location, status)
VALUES ('Festival Lyon 2026', '2026-09-03', '2026-09-06', 'Lyon', 'programmé');
```

La clé primaire id, auto-incrémentée, est attribuée automatiquement.

Question 25

```
SELECT id FROM events WHERE status = 'programmé';
```

Question 26

Il faut mettre à jour l'attribut stand_id de la table terminals. Dans la ligne du terminal concerné (repéré par son terminal_uid), stand_id reçoit la valeur de la clé primaire id du stand snack 3 du festival, c'est-à-dire le stand de la table stands dont event_id est égal à la clé primaire obtenue à la question 25.

PARTIE 2 – CONCEPTION D'UN SYSTÈME INFORMATIQUE

Question 27

Le pare-feu ASA 5506 crée la DMZ grâce à l'attribution d'un niveau de sécurité à chaque interface (de 0 à 100, plus le niveau est élevé plus le réseau est considéré comme fiable), à l'utilisation de trois interfaces (outside, dmz1, inside) et à la mise en œuvre de listes de contrôle d'accès (ACL) et de la traduction d'adresses (NAT) pour une DMZ à trois interfaces (DT4).

Question 28

Interface	Nom	Adresse	Masque	Adresse réseau
GigabitEthernet1/1	outside (niveau 0)	96.31.56.253	255.255.255.252 (/30)	96.31.56.252
GigabitEthernet1/2	dmz1 (niveau 50)	192.168.1.1	255.255.255.0 (/24)	192.168.1.0
GigabitEthernet1/3	inside (niveau 100)	192.168.0.1	255.255.255.0 (/24)	192.168.0.0

Le masque 255.255.255.252 correspond à un réseau de 4 adresses ; 253 appartient au bloc 252 à 255, d'où l'adresse réseau 96.31.56.252.

Question 29

Chaque sous-réseau doit contenir au plus 30 machines (terminaux et passerelle). Un masque /27 offre 30 adresses utilisables, ce qui convient. Le réseau 192.168.69.0/24 est découpé en blocs de 32 adresses : 192.168.69.0, .32, .64, .96, .128, .160, .192, .224. Le VLAN 10 utilise le premier sous-réseau, le VLAN 20 le deuxième, le VLAN 99 le dernier.

Sous-réseau	Masque CIDR	Plage des terminaux (DHCP)	Passerelle par défaut	Broadcast
VLAN 10 : 192.168.69.0	/27 (255.255.255.224)	192.168.69.1 à 192.168.69.29	192.168.69.30	192.168.69.31
VLAN 20 : 192.168.69.32	/27 (255.255.255.224)	192.168.69.33 à 192.168.69.61	192.168.69.62	192.168.69.63
VLAN 99 : 192.168.69.224	/27 (255.255.255.224)	192.168.69.225 à 192.168.69.253	192.168.69.254	192.168.69.255

La dernière adresse utilisable de chaque sous-réseau est réservée à la passerelle par défaut.

Question 30

Élément	Couche OSI
SSID	2 – Data Link (liaison de données, Wi-Fi)
HTTPS	7 – Application (TLS assurant le chiffrement entre les couches 4 et 7)
Sous-réseau	3 – Network (réseau, adressage IP)
VLAN	2 – Data Link (liaison de données, segmentation de la trame Ethernet)

Question 31

Sur la figure 5 (sujet au format A4), la barre d'échelle de 100 m mesure environ 3,7 cm. AP2 et le PGR sont distants d'environ 6,8 cm, soit 6,8 × 100 / 3,7 ≈ 184 m : environ 185 m (entre 180 et 190 m).

Cette distance dépasse 100 m : la liaison RJ45 en cuivre (100 m maximum) et le Wi-Fi (environ 30 à 100 m) sont exclus. D'après DT5, les technologies possibles sont la fibre optique multimode (jusqu'à 300 m) et la fibre optique monomode (jusqu'à 80 km).

Question 32

La liaison PGR – AP2 est en fibre multimode (DOC11) : un module SFP MGBSX1 (1000BASE-SX, multimode) à chaque extrémité, un convertisseur fibre/RJ45 côté AP2 (AP2 n'a qu'une prise RJ45) et, côté PGR, un switch disposant de ports SFP 1G.

Nom	Réf	Nombre	Prix unitaire (HT)	Prix total (HT)
Convertisseur	5618	1 lot	35,82 €	35,82 €
Switch	S3410-24TS-P	1	968,00 €	968,00 €
Module SFP	MGBSX1	2	7,00 €	14,00 €
Total (HT)				1 017,82 €
TVA 20 %				203,56 €
Total (TTC)				1 221,38 €

Le S3910-24TS (619 €) n'a aucun port SFP 1G (ligne « Ports SFP : – » dans DT6) et ne peut pas recevoir le module MGBSX1. Le S3410-24TS-P est le switch le moins cher disposant de ports SFP 1G (2 ports combo), le PoE n'étant pas un critère de choix. Le coût total de la partie étudiée est de 1 017,82 € HT, soit 1 221,38 € TTC.

Question 33

```
INSERT INTO quantities (value, unit)
VALUES (25, 'cL'), (33, 'cL'), (50, 'cL');
```

La clé primaire id, auto-incrémentée, n'est pas renseignée.

Question 34

Équipement	Adresse IPv4	Port
Terminal de paiement (client)	192.168.0.1	60714
RPI (serveur du stand autonome)	192.168.0.2	8080
Serveur d'applications	Cases barrées, sans objet	

Valeurs relevées sur la figure 14 (adresses en tête des colonnes, ports sur chaque ligne).

Question 35

Figure 14 (lignes 27 à 41)	N° ligne (début phase)	N° ligne (fin phase)	N° ligne
Phase de connexion de TCP (SYN, SYN-ACK, ACK)	27	29	
Séquence où commence WS			32
Acquittement TCP du RPI			31
Acquittement TCP du terminal			33

Ligne 32 : HTTP/1.1 101 Switching Protocols (la première trame WebSocket est en ligne 34). Ligne 31 : 8080 → 60714 [ACK] ; les lignes 35 et 39 sont aussi acceptées. Ligne 33 : 60714 → 8080 [ACK] ; les lignes 29, 37 et 41 sont aussi acceptées.

Question 36

Dans la trame WebSocket, le deuxième octet 0xA8 indique un masquage (bit b7 = 1) et une longueur de payload de 0x28 = 40 octets. Les 4 octets de masquage sont ceux qui suivent cet octet de longueur : 1d aa c3 26.

Le masque est donc 0x1D 0xAA 0xC3 0x26.

Payload : 66 88 b5 49 | 71 df ae 43 | 42 c9 af 04 | 27 9f f3 0a … Le masque s'applique en boucle par groupes de 4 octets (DT7) : les octets 13 à 16 (27 9f f3 0a) sont masqués par 1d aa c3 26, donc le 14e octet (0x9F) est associé au 2e octet du masque (0xAA) et le 15e (0xF3) au 3e (0xC3).

Démasquage : 0x9F ⊕ 0xAA = 0x35 (caractère « 5 ») ; 0xF3 ⊕ 0xC3 = 0x30 (caractère « 0 »).

Le volume demandé est donc de 50 cL (valeur « 50 »). Le payload démasqué complet est {"volume_cl":50,"duree_distribution":60}.

Question 37

La commande est validée par la trame 17 à 10,8429 s (volume_cL 25). La réponse du distributeur indiquant la fin de distribution est la trame 19 à 17,3985 s (status_code 1).

Durée de remplissage : 17,3985 – 10,8429 = 6,5556 s, soit environ 6,56 s.

6,56 s est inférieur à 11 s : la durée maximale fixée par le cahier des charges est respectée pour un verre de 25 cL.

Question 38

Nombre d'impulsions pour 25 cL : 250 mL / 2,5 mL = 100 impulsions.

En 11 s, la fréquence des impulsions vaut f = 100 / 11 ≈ 9,1 Hz. Sur la figure 16, le taux de détection est de 100 % jusqu'à 200 Hz : toutes les impulsions sont comptées, donc la durée de 11 s peut être respectée.

Question 39

500 mL / 2,5 mL = 200 impulsions. La fréquence maximale pour 100 % de réussite est de 200 Hz (figure 16), d'où t_{min} = 200 / 200 = 1 s.

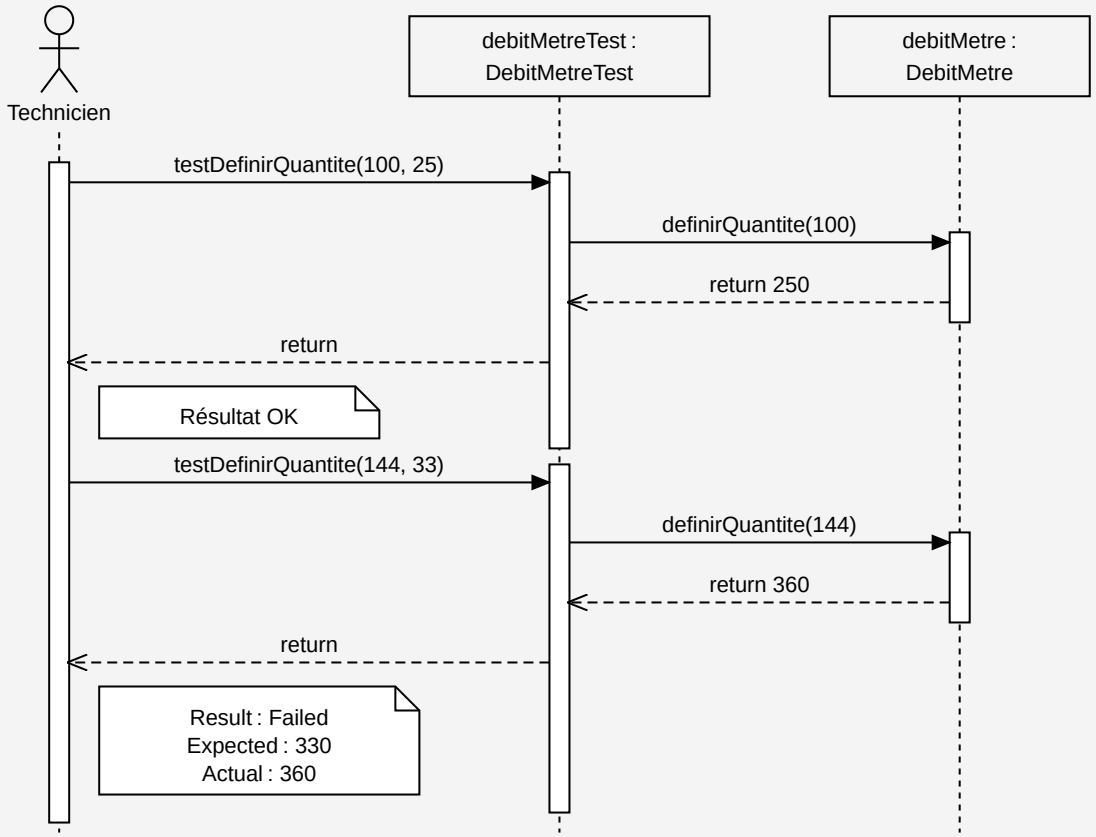
Question 40

La méthode est + demandeDcy() : void, qui est publique. Ihm est associée à Cycle par l'association navigable « cycle » (multiplicité 1) : Ihm y a donc accès.

Question 41

L'attribut - compteur : int de CompteurImpulsion est privé. De plus, Ihm n'a aucune association avec CompteurImpulsion : Ihm n'y a donc pas accès.

Question 42



DR-Pro13 complété (format DT8)

Le second test échoue car 144 impulsions × 2,5 mL = 360 mL, alors que 330 mL (33 cL) sont attendus.

Question 43

La communication individuelle prévue par l'article 34 du RGPD (DT9) n'est obligatoire que si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. L'injection SQL n'a touché que la table user_event_roles, qui contient les identifiants de rôles (user_id, event_id, role) et non les données d'identité (lastname, firstname, email, password_hash de la table users) ni les données des bracelets (solde, identifiants NFC).

La société CISS n'est donc pas tenue de communiquer auprès de l'ensemble des festivaliers et des bénévoles. Seules les personnes dont les rôles ont été touchés (organisateurs, techniciens, superviseurs ou bénévoles concernés) peuvent être concernées, et seulement si le risque est jugé élevé. Le user_id reste une donnée personnelle indirecte, mais l'atteinte à des seules informations de

rôle ne présente pas, en l'état, de risque élevé au sens du paragraphe 1 ; la notification à la CNIL (article 33) reste en revanche à examiner.

PARTIE 3 – VALIDATION DU CHOIX DU DÉBITMÈTRE

Question 44

Sur la figure 19, les impulsions apparaissent à 20, 50 et 80 ms, d'où $\Delta T_{\min} = 50 - 20 = 30\ \text{ms}$.

Question 45

$N_{I1} = \dfrac{3600}{\Delta T_{\min}} = \dfrac{3600}{0{,}030} = 120\,000$ impulsions.

Question 46

D'après la figure 20, l'OF-10 ZZT délivre 2,5 cm³ par impulsion.

$D_{\max} = N_{I1} \times 2{,}5 = 120\,000 \times 2{,}5 = 300\,000\ \text{cm}^3/\text{h}$, ce qui correspond au débit maximum exigé (300 000 cm³/h).

Question 47

$N_{I2} = \dfrac{250}{2{,}5} = 100$ impulsions.

Question 48

Sur la figure 21, les deux impulsions sont à environ 10 ms et 97 ms : $\Delta T_{\max} \approx 97 - 10 = 87\ \text{ms}$.

$T_{\max} = N_{I2} \times \Delta T_{\max} = 100 \times 0{,}087 \approx 8{,}7\ \text{s}$.

Question 49

- Débit maximum : le débitmètre mesure jusqu'à 300 000 cm³/h, valeur exigée par le cahier des charges.
- Durée de remplissage : $T_{MAX} \approx 8{,}7$ s < 11 s pour un verre de 0,25 L.

Les deux critères sont vérifiés : le débitmètre OF-10 ZZT convient.

PARTIE 4 – DÉTECTION DES FÛTS DE BOISSON VIDES

Question 50

La branche R1–R2 est alimentée par E. Par diviseur de tension : U1 = E × R1 / (R1 + R2).

Question 51

Loi des mailles : $U_1 + \Delta U - U_4 = 0$, d'où $\Delta U = U_4 - U_1$, avec $U_4 = E \times \dfrac{R_4}{R_3 + R_4}$.

Question 52

Quantum : $q = \dfrac{U_{PE}}{2^{24}} = \dfrac{5{,}00}{16\,777\,216} = 2{,}98 \times 10^{-7}$ V, soit environ 0,298 µV.

Question 53

L'amplificateur de la figure 24 a un gain de 130 : $U_{a,\text{alerte}} = 130 \times 6{,}8 \times 10^{-3} = 0{,}884$ V.

Question 54

$$N_{\text{alerte}} = \frac{U_{a,\text{alerte}}}{q} = \frac{0{,}884 \times 2^{24}}{5{,}00} = 2\,966\,211{,}8$$

Le CAN donne la partie entière : $N_{\text{alerte}} = 2\,966\,211$. Remarque : avec q arrondi à 2,98 × 10^{-7} V, on obtient environ 2 966 443, écart dû uniquement à l'arrondi de q ; cette valeur est également acceptée.

Question 55

Une résolution de 2 kg correspond à $\Delta U = 2\ \text{mV}$, soit $U_a = 130 \times 2 \times 10^{-3} = 0{,}26$ V en entrée du CAN.

Le quantum q = 0,298 µV correspond à une masse $\dfrac{2{,}98 \times 10^{-7}}{130 \times 10^{-3}} \approx 2{,}3 \times 10^{-6}$ kg, soit environ 2,3 mg : la résolution de 24 bits est donc suffisante.

Elle n'est pas judicieuse : $5{,}00 / 0{,}26 \approx 19{,}2$, soit 20 niveaux nécessaires ; 5 bits ($2^5 = 32$ niveaux) suffisent. Le CAN est surdimensionné, ce qui augmente le coût inutilement.

PARTIE 5 – CARACTÉRISATION DU PROTOCOLE DE COMMUNICATION NFC

Question 56

Sur la figure 26 (calibre 10 µs/div), chaque bit occupe environ 0,94 division : $T_B \approx 0{,}94 \times 10 \approx 9{,}4\ \mu\text{s}$.

Question 57

$$D = \frac{1}{T_B} = \frac{1}{9{,}4 \times 10^{-6}} \approx 106\ \text{kbit/s}.$$

Question 58

Codage de Miller modifié : un 1 présente une pause au milieu du bit ; un 0 qui suit un 0 présente une pause en début de bit ; un 0 qui suit un 1 ne présente pas de pause.

Bit	b0	b1	b2	b3	b4	b5	b6	b7
Observation	pause en début	pause en début	pause au milieu	pas de pause (après un 1)	pause en début	pause au milieu	pas de pause (après un 1)	pause au milieu
Valeur	0	0	1	0	0	1	0	1

Octet transmis : {b7, b6, b5, b4, b3, b2, b1, b0} = {1, 0, 1, 0, 0, 1, 0, 0}.

Question 59

b7 à b1 = 1010010, ce qui correspond dans la figure 27 à '52' = WUPA : commande envoyée pour réveiller un tag.

Question 60

Sur la figure 28 (centre 13,5 MHz, span 1 MHz, soit 100 kHz/div), le pic est situé environ 0,6 division à droite du centre : $f_{\text{porteuse}} \approx 13{,}5 + 0{,}6 \times 0{,}1 \approx 13{,}56\ \text{MHz}$.

Question 61

La fréquence porteuse mesurée (13,56 MHz) et le débit calculé (106 kbit/s) sont conformes à la norme ISO/IEC 14443 type A : la communication entre le lecteur et le tag est valide.

PARTIE 6 – CHOIX DES ANTENNES

Question 62

FSL = –147,5 + 20 log(5,54 × 10^9) + 20 log(65)

20 log(5,54 × 10^9) = 194,87 dB ; 20 log(65) = 36,26 dB.

FSL = –147,5 + 194,87 + 36,26 = 83,63 dB, soit environ 84 dB.

Question 63

La sensibilité du terminal est $S_{TER} = -67\ \text{dBm}$; la marge de 10 dB impose $P_{TER\,\min} = -67 + 10 = -57\ \text{dBm}$.

Question 64

Bilan de l'AP vers le terminal : $P_{TER\,\min} = P_{AP} + G_{APMIN1} + G_{TER} - \text{FSL}$.

$G_{APMIN1} = P_{TER\,\min} - P_{AP} - G_{TER} + \text{FSL} = -57 - 23 - 0 + 84 = 4\ \text{dBi}$.

Question 65

$\text{PIRE} = P_{AP} + G_{APMAX}$ (sans pertes de câble). Avec PIRE = 30 dBm et P_{AP} = 23 dBm :

$G_{APMAX} = 30 - 23 = 7\ \text{dBi}$.

Question 66

Critères : la liaison étant bidirectionnelle, le gain doit être au moins égal à max(4 ; 6) = 6 dBi (figures 29 et 30) et au plus égal à 7 dBi ; la bande doit couvrir 5 500 MHz (AP1) et 5 540 MHz (AP2) ; l'ouverture doit être au moins égale à 235° pour AP1 et à 20° pour AP2 (figure 31).

- AP1 : seule l'AIR-ANT2547-VN convient (7 dBi, 360°, 5150-5875 MHz). La 2568-VG (8 dBi) dépasse la PIRE autorisée.
- AP2 : l'AIR-ANT5170-PR (7 dBi, 70°, 5150-5850 MHz), directive et adaptée, ou l'AIR-ANT2547-VN conviennent.
- Exclues : la 2466-PR (bande 2,4 GHz), la 2588-P3M (8 dBi) et la 5114-P2M (14 dBi).

Continue à t'entraîner

Retrouve tous les sujets et corrigés du BTS CIEL, classés par épreuve et par année :
coursbtsciel.fr/annales-sujets-et-corriges

Pour réviser tout le programme avant l'examen, les Fiches de Révision du BTS CIEL reprennent l'essentiel de chaque épreuve :
coursbtsciel.fr/fiches-de-revision

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.