

CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C – Session 2017 -

CONCOURS INTERNE

Epreuve Ecrite Obligatoire

CONNAISSANCES AERONAUTIQUES

Date de l'épreuve : 27 juin 2017
Durée de l'épreuve : 3 heures
Coefficient : 5 (concours interne)

CALCULATRICE INTERDITE

Ce sujet comporte :

- ➡ une page de garde
- ➡ une page d'instructions aux candidats,
- ➡ cinq pages de questions (12 questions),
- ➡ une page mentionnant le barème

INSTRUCTIONS AUX CANDIDATS

EPREUVE OPTIONNELLE DE CONNAISSANCES AERONAUTIQUES

Consignes

- Rédigez les réponses directement dans le sujet à la suite de chaque question, dans les emplacements en pointillés prévus à cet effet. Utilisez un stylo à bille ou feutre à pointe fine noir ou bleu. L'usage du crayon papier est interdit
- L'épreuve est notée sur 20
- Un tableau du barème de points est en annexe

Identification :

- N'oubliez pas de reporter votre numéro d'inscription de table dans le cadre prévu à cet effet.

CONCOURS TSEEAC CEAPF INTERNE
SESSION 2017
EPREUVE OBLIGATOIRE OPTIONNELLE
CONNAISSANCES AERONAUTIQUES
SUJET 1

- 1) On appelle « échelle d'une carte », le rapport :

.....
.....
.....

- 2) Expliquez la différence entre la route et le cap.

.....
.....
.....

Que déduisez-vous d'un vol se déroulant par vent nul ?

.....
.....

Comment souffle le vent par rapport au cap et à la route ?

.....
.....

- 3) Vous désirez suivre une route vraie de 190° . La déclinaison est de $8^\circ W$. Vous savez que sur la route, l'avion a une dérive de 15° gauche. Quel est le cap magnétique à suivre ?

.....
.....
.....

- 4) Votre avion vole à une vitesse de 100 kts sans vent. Combien de temps mettez-vous pour parcourir 50 NM ?

.....
.....

- 5) Dans quelle gamme de fréquences fonctionne le VOR ? et qu'est-ce qui pourrait gêner la propagation/réception de ces ondes radio ?

.....
.....
.....

Et par temps orageux, le fonctionnement du VOR est-il moins performant ? Pourquoi ?

.....
.....

Par rapport à quel nord sont calculées les indications du VOR ?

.....

Pour une approche aux instruments basée sur un VOR. De quel type d'approche s'agit-il ?
Et, que représente le VOR dans le cas où l'approche débute à sa verticale ?

.....
.....

En couplant le VOR avec un DME, combien y-a-t-il de segments d'approche ? Lesquels ?

.....
.....

Expliquez, pourquoi et à partir de quel moment l'avion en segment final termine par une API ?

.....
.....
.....
.....

Quels sont les deux critères de minima opérationnel d'une approche aux instruments classique mentionnés sur la carte IAC ?

.....
.....

Après l'API, le CDB décide de faire une attente en attendant l'amélioration des conditions météorologiques. Combien de types d'entrée dans une attente y-a-t-il ? Lesquels ?

.....
.....

6) En volant sous le cumulonimbus qui est un nuage dangereux pour l'aéronautique, quels sont les phénomènes que l'on peut rencontrer ?

.....
.....
.....

7) Comment souffle la brise de mer qui est un vent local des régions côtières ?

.....
.....

8) Pour mesurer le vent sur un aéroport, où sont installés la girouette et l'anémomètre, et à quelle hauteur du sol ?

.....
.....

- 9) Sur un aérodrome contrôlé, la piste est orientée 250°/070° par rapport au nord géographique. La déclinaison magnétique est de 5°W. Quels sont les deux QFU, et l'identification des pistes associées ?

.....

.....

.....

Les conditions sont VMC. Vent 160°/10 kts, QNH = 1016 Hpa, altitude de la piste 56 ft.

TA (altitude de transition) = 3000 ft.

Un monomoteur PA 28, au parking, met en route pour quelques tours de piste initialement. Quelle est la piste en service ? et que doit faire le pilote pour remonter la piste et s'aligner ?

.....

.....

.....

Lors du premier tour de piste, le pilote s'aperçoit que son calage altimétrique est resté sur le QNH. S'agissant d'un circuit de piste standard, à quelle altitude / QNH doit-il stabiliser en vent arrière ?

.....

.....

.....

Après deux tours, le pilote décide d'aller vers l'Ouest, en stabilisant à 400 ft/QNH au-dessus de l'océan pour une distance de 15 NM environ. Que pensez-vous de son altitude de vol et de son éloignement des côtes ? justifiez.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Finalement, le pilote préfère faire demi-tour et met le cap vers l'Est à 4500 ft/QNH au-dessus du lagon. Est-ce que le niveau est approprié suivant les différentes règles ? Justifiez.

.....

.....

.....

.....

.....

Une quinzaine de minutes plus tard, le CDB décide de revenir vers l'aérodrome en amorçant sa descente pour survoler le point culminant des reliefs, côté à 2000 ft. Il souhaite passer à 1000 ft au-dessus. Quel est le calage altimétrique approprié pour le franchissement des obstacles et des reliefs ? Pourquoi ?

.....

.....

.....

.....

.....

De retour dans la CTR de classe D, le contrôleur informe que la visibilité est de 3000 m et le plafond à 1600 ft dans la circulation d'aérodrome. Que pouvez-vous en déduire ? Précisez.

.....

.....

.....

.....

.....

A l'approche de la circulation d'aérodrome, le contrôleur informe le monomoteur qu'un IFR s'apprête à décoller de la piste en service. Quelle est sa responsabilité vis-à-vis de ces deux aéronefs ? Précisez.

.....

.....

Peu de temps après le décollage de l'IFR, les deux trafics sont séparés. Le PA28 arrive en début de vent arrière. Il annonce « panpan, panpan, panpan » précisant que le moteur a des ratés. Que doit faire le contrôleur ?

.....

.....

Finalement le monomoteur se pose sans encombre à 04h15 UTC, dix minutes après l'heure du coucher de soleil. Quelle action doit entreprendre le contrôleur ?

.....

.....

Nous sommes en Polynésie française, dans ce cas présent, la nuit aéronautique débute à quelle heure et pour se terminer quand ?

.....

.....

Si l'avion avait prévu d'arriver à 04h35 UTC dans les mêmes conditions, aurait-il pu bénéficier d'une clairance de VFR spécial ? Pourquoi ?

.....

.....

.....

Arrivé au parking, que lit le pilote sur son altimètre calé cette fois-ci sur le QFE ? Le QNH n'ayant pas varié depuis le décollage, quelle est la valeur du QFE ?

.....
.....
.....

Pour terminer, le contrôleur a relevé les paramètres météo suivants pour les transmettre au prochain vol dont l'ETA est dans 15 minutes environ :

QNH = 1018, QFE = 1016, Vent 080°/12 kts, Epars 2000 ft, Vis 10 km, température = 28°C et la piste en service.

Mettez ces paramètres dans l'ordre pour la transmission aux usagers

.....
.....

10) De quoi est constituée la cellule d'un avion ?

.....
.....
.....

11) Quelle est la traînée totale d'un avion ?

.....
.....

12) Quelle est la gouverne primaire d'inclinaison ?

.....
.....



CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C – Session 2017 -

CONCOURS EXTERNE/INTERNE
Épreuve optionnelle obligatoire

SCIENCES DE L'INGENIEUR

Date de l'épreuve : 27 juin 2017

Durée de l'épreuve : 3 heures

Coefficient : 6 (concours externe)
5 (concours interne)

Ce sujet comporte : 2 Dossiers

- ⇒ Une page de garde
- ⇒ Une page de consignes (page 1)
- ⇒ Un dossier sujet : 23 questions QCM (pages 2 à 8)
- ⇒ Un dossier technique (pages 1 à 13)

CALCULATRICE INTERDITE

SCIENCES DE L'INGENIEUR

SUJET

INSTRUCTIONS AU CANDIDAT

Avertissement

- De nombreuses questions sont indépendantes.
- Certaines questions peuvent avoir plusieurs réponses possibles mais toutes en ont au moins une.
- Les réponses fausses seront pénalisées.
- Vous devez cocher la ou les bonnes réponses de façon claire et sans ambiguïté, pas de ratures ni « blancotage ».

Instructions pour l'utilisation de la grille-réponse :

- Complétez la grille-réponse à l'aide d'un stylo à bille ou feutre à pointe fine noir ou bleu. L'usage du crayon papier est interdit ;
- Il ne vous est délivré qu'une seule grille réponse, retranscrivez vos réponses après vous être relu(e) soigneusement ;
- Sur la grille-réponse, tracez une croix dans la case correspondant à votre choix ;
- Si vous désirez modifier une réponse, noircissez complètement la case et tracez une croix au nouvel emplacement. Exemple :

Questions \ Réponses	2
A	
B	
C	
D	

Identification :

N'oubliez pas de reporter votre numéro d'inscription de table sur la grille-réponse.

Documents

- Dossier technique 13 pages

Généralités :

1. Le degré de sécurité S3 de la norme DIN 32757 concerne :
 - ☐ A : la protection des personnes lors de l'ouverture de la corbeille
 - ☐ B : la préservation de la confidentialité après destruction des documents
 - ☐ C : la dimension maximale des bandes de papier après destruction
 - ☐ D : la dimension minimale des bandes de papier après destruction

2. La norme DIN 32757 est une norme :
 - ☐ A : de l'aviation civile
 - ☐ B : de la « National Security Agency » américaine
 - ☐ C : française
 - ☐ D : allemande du « Deutsches Institut für Normung »

3. La capacité de destruction en nombre de feuille par minute est :
 - ☐ A : 5
 - ☐ B : 10
 - ☐ C : 20
 - ☐ D : 40

4. La vitesse de défilement des feuilles est 3,2m/min, combien de longueur de feuille A4 peut-on faire passer en 1 minute :
 - ☐ A : 5
 - ☐ B : 10
 - ☐ C : 20
 - ☐ D : 40

Technologie :

5. Le moteur d'entraînement des couteaux est un moteur universel. Cela signifie qu'il peut théoriquement fonctionner :
 - ☐ A : uniquement en alternatif
 - ☐ B : uniquement en continu
 - ☐ C : indifféremment en alternatif ou continu
 - ☐ D : indifféremment en monophasé ou triphasé

6. Le moteur universel est, de par sa constitution, un moteur :
- ☐ A : à courant continu à excitation série
 - ☐ B : à courant continu à excitation parallèle
 - ☐ C : un moteur asynchrone
 - ☐ D : un moteur synchrone
7. L'inversion du sens de rotation entre la position « auto » et « déburrage » est obtenue par :
- ☐ A : un interrupteur à glissière
 - ☐ B : par inversion des sens relatifs des courants dans l'induit et l'inducteur
 - ☐ C : il n'y a pas d'inversion de sens
 - ☐ D : par inversion du courant dans l'inducteur
8. La puissance indiquée pour le moteur est sa :
- ☐ A : puissance électrique
 - ☐ B : puissance utile
 - ☐ C : puissance mécanique
 - ☐ D : puissance absorbée

La présentation du destructeur stipule « 2mn ON/30mn OFF »

En supposant que l'utilisateur respecte cette consigne et que le rendement du moteur soit de 0,5 :

9. Quelle est l'énergie électrique absorbée par le moteur en une heure ?
- ☐ A : 72000J
 - ☐ B : 20Wh
 - ☐ C : 3,6kVA
 - ☐ D : 0,15 kWh
10. La transmission de puissance est assurée par des engrenages, combien y a-t-il d'engrenages entre le moteur et le rouleau moteur:
- ☐ A : 3
 - ☐ B : 4
 - ☐ C : 5
 - ☐ D : 6

11. Quelle est la fonction du réducteur à engrenages :

- ☐ A : augmenter la puissance
- ☐ B : augmenter le couple
- ☐ C : augmenter le rendement
- ☐ D : augmenter l'énergie

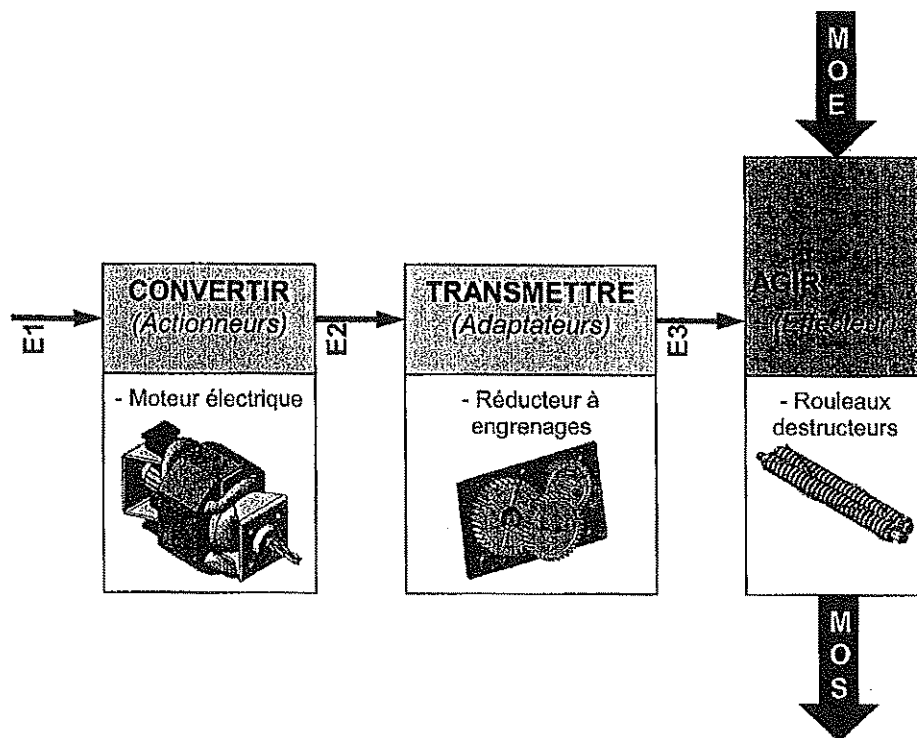
12. Les engrenages à dentures droites sont appréciés pour :

- ☐ A : son faible coût
- ☐ B : sa puissance
- ☐ C : sa mise en œuvre simple
- ☐ D : sa résistance

13. Le moteur électrique dispose sur son axe un pignon à dentures :

- ☐ A : droite
- ☐ B : inclinée
- ☐ C : hélicoïdale
- ☐ D : elliptique

Chaîne d'énergie:



14. Quelle est la nature de l'énergie repérée E2 :

- ☐ A : énergie électrique
- ☐ B : énergie mécanique
- ☐ C : énergie électromagnétique
- ☐ D : énergie éolienne

En supposant qu'il y a roulement sans glissement entre les rouleaux et les feuilles, la vitesse de défilement des feuilles est $v=2,1$ m/min en pleine charge. Le diamètre des rouleaux est $D=23$ mm.

15. Quelle est la vitesse de rotation des rouleaux :

- ☐ A : 24,15 tr/min
- ☐ B : 1,74 tr/min
- ☐ C : 29 tr/min
- ☐ D : 3,04 tr/min

16. Quelle est le rapport de transmission globale $r = \frac{N_{\text{rouleau}}}{N_{\text{moteur}}}$:

- ☐ A : 194,25
- ☐ B : 0,00514
- ☐ C : 3,71
- ☐ D : 0,2695

17. En déduire la vitesse de rotation du moteur électrique :

- ☐ A : 5654 tr/min
- ☐ B : 1285 tr/min
- ☐ C : 14172 tr/min
- ☐ D : 25000 tr/min

En supposant le couple résistant sur le rouleau moteur vaut 30N.m, et que le rendement de la transmission par engrenages est de 65%,

18. Quelle est la puissance utile du moteur :

- ☐ A : 46W
- ☐ B : 91,2W
- ☐ C : 140W
- ☐ D : 150W

19. Dans ces conditions, le moteur consomme un courant de 1,5A sous une tension de 220V, quelle est la puissance absorbée par le moteur:

- ☐ A : 440W
- ☐ B : 330W
- ☐ C : 184W
- ☐ D : 150W

20. En déduire le rendement global de la chaîne d'énergie (moteur+réducteur):

- ☐ A : 9%
- ☐ B : 27.6%
- ☐ C : 53%
- ☐ D : 65%

Vérification de la roue 8 :

On désire vérifier le dimensionnement de la roue 8 qui transmet le couple utile aux rouleaux. Une simulation informatique a donné les résultats ci-dessous :

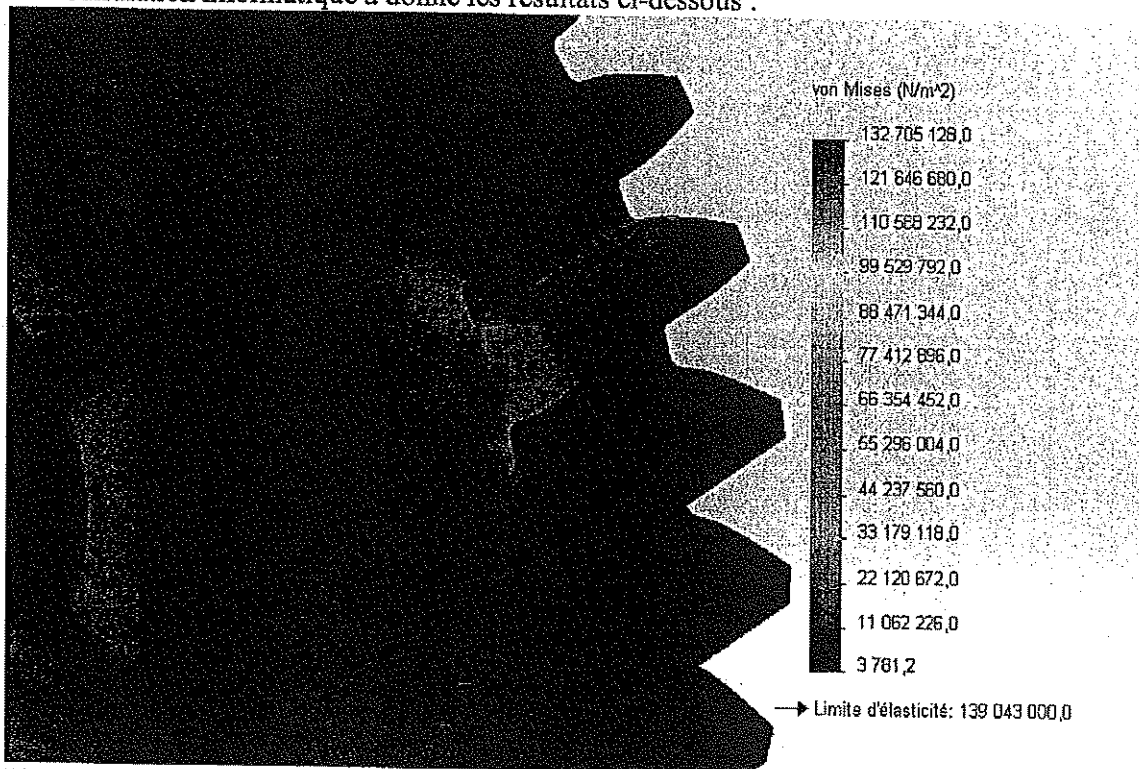


Fig. Simulation RDM

21. En vous aidant de la figure ci-dessus, la contrainte maximale est :

- ☐ A : 139 MPa
- ☐ B : 1327 bars
- ☐ C : 3781 MPa
- ☐ D : 132705128 MPa

22. En déduire le coefficient de sécurité effectif

- ☐ A : 1,05
- ☐ B : 9,5
- ☐ C : 7
- ☐ D : 0,95

Chaîne d'information :

23. Ouvrir la corbeille pendant le fonctionnement est il dangereux ?

- ☐ A : non tant que le détecteur "présence corbeille" fonctionne correctement
- ☐ B : non l'utilisateur ne pouvant avoir accès aux couteaux
- ☐ C : non car l'ouverture de la corbeille est verrouillée pendant le fonctionnement
- ☐ D : oui, potentiellement

N° CANDIDAT :

Document réponses à rendre

Question	A	B	C	D
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				

SCIENCES DE L'INGENIEUR

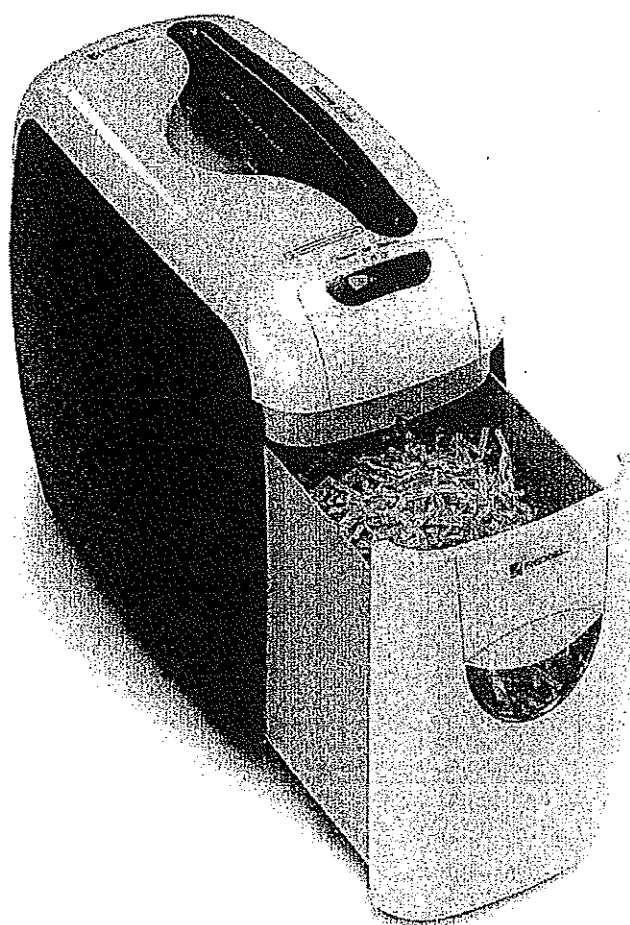
DOSSIER TECHNIQUE

Ce dossier technique comporte : **13 pages**

DESTRUCTEUR de DOCUMENTS

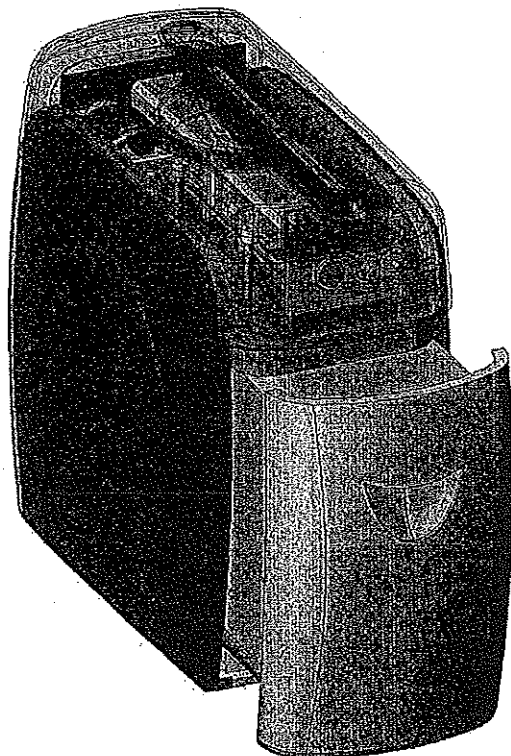
REXEL "Style"

DOCUMENTATION TECHNIQUE



Présentation générale :

Le destructeur de document Rexel « Style » fait parti d'une gamme de destructeurs pour le bureau à domicile. Sa taille compacte et son design ultramoderne font de lui le produit le plus contemporain du marché. Il peut être utilisé pour un usage régulier.



Caractéristiques techniques :

- | | |
|--|---|
| <ul style="list-style-type: none">- Destructeur à coupe croisée en particules de 4 x 35 mm- Détruit 5 feuilles (80 g/m²) à la fois et les cartes de crédit- Niveau de sécurité S3 selon la norme DIN 32757- Ouverture de coupe 225 mm- Vitesse de destruction : 3,2 m/min ; soit environ 40 feuilles A4 par minute- Marche & Arrêt automatiques- Marche arrière en cas de bouchage- Niveau sonore : inférieur à 70 décibels- Cycles de fonctionnement : 2 min « ON » / 30 min « OFF » | <ul style="list-style-type: none">- Arrêt automatique de sécurité corbeille sortie- Sécurité thermique anti-surchauffe- Corbeille de 7,5 litres extractible (soit plus de 50 feuilles A4 80gr.)- Dimensions de l'appareil / Masse : 340 x 185 x 320 mm / 3.8 kg- Fenêtre permettant de visualiser le niveau de remplissage de la corbeille- Tension / Fréquence nominale : 220 – 240 V ~50 Hz- Intensité nominale : 0.8 A- Puissance : 150 Watts- Garantie retour atelier : 2 ans |
|--|---|

Mode d'emploi :

Notice d'utilisation des Rexel Prostyle, Style+ et Style

F

Veuillez lire attentivement ces instructions avant d'utiliser l'appareil.

Introduction

Merci d'avoir choisi ce destructeur Rexel qui devrait vous donner entière satisfaction. Veuillez prendre quelques minutes pour lire le mode d'emploi qui vous indiquera comment profiter au maximum de votre nouvel appareil.

Consignes de sécurité

1. Veuillez conserver ces instructions dans un lieu sûr pour toute référence ultérieure.
2. Prenez une attention toute particulière aux symboles de sécurité illustrés sur la face supérieure du destructeur et observez-les lors du fonctionnement de l'appareil.
3. Si le destructeur a besoin d'être nettoyé, débranchez-le de la prise de courant et utilisez un chiffon humide. N.B. : N'utilisez jamais de produit de nettoyage à cet effet.
4. Ne placez pas l'appareil dans un endroit humide.
5. Ne placez pas l'appareil dans un endroit humide.
6. Veillez à ne pas renverser de liquide sur l'appareil.
7. Remplacez le produit et une preuve d'achat (ticket de caisse) au magasin où vous l'avez acheté dans les cas suivants :
 - l'appareil fonctionne mal depuis qu'un liquide a été accidentellement déversé sur la machine ;
 - le destructeur ne fonctionne pas, bien que vous ayez suivi les instructions de cette notice.
8. Veillez à ce que personne ne puisse bricoler sur le cordon d'alimentation.
9. Veuillez vous assurer que l'alimentation est compatible avec les exigences de l'appareil (220-240 V 50 Hz).
10. Pour éviter tout risque de blessure, n'ouvrez pas la boîte de l'appareil pour essayer d'effectuer vous-même une réparation. La garantie sera annulée en cas de tentative de réparation par du personnel non qualifié.

Description des pièces du produit (fig 1)

- A. Cordon d'alimentation (schéma européen illustré)
- B. Poignée de contrôle du remplissage de la corbeille
- C. Ouverture de coupe

Préparation avant l'emploi

Comment utiliser le destructeur correctement :

1. Veillez à ne pas insérer de doigts, cravates ou autres objets dans l'ouverture de coupe du destructeur.
2. Pour éviter d'endommager les couteaux, essayez de ne pas faire passer de trombones, agrafes, matières plastifiées et sacs en plastique, par exemple, dans le destructeur.
3. N'alimentez pas de feuilles de papier humides car elles risquent de s'enchevêtrer dans les couteaux.
4. Lors de l'alimentation des feuilles, ne dépassez pas la capacité de coupe indiquée.
5. N'utilisez que l'ouverture de coupe continue pendant plus de 3 minutes. S'il fonctionne pendant trop longtemps, le moteur risque de surchauffer.
6. N'utilisez la fonction « REV » (<C>) (marche arrière) qu'en cas de bouchon. L'emploi excessif de cette fonction peut, en effet, empêcher le blocage des documents dans l'ouverture de coupe, ce qui aura un effet néfaste sur le bon fonctionnement du destructeur.

Procédure de fonctionnement (fig 2)

1. Branchez l'appareil sur une prise de courant alternatif.
2. Vérifiez que la corbeille du destructeur est bien positionnée à l'intérieur du destructeur.
3. Faites glisser le commutateur dans la position ON/AUTO (mode veille).
4. En cas de non utilisation, faites glisser le commutateur dans la position O (hors tension).

Alimentation et arrêt automatiques

- Placez le document ou le sac de crottin au centre de l'ouverture de coupe et la destruction se lance automatiquement (fig 3).
- Les feuilles d'une largeur inférieure à celle du format A4 doivent être placées au milieu de l'ouverture de coupe pour garantir le fonctionnement automatique du destructeur.
- Les couteaux s'arrêtent de tourner automatiquement dès la fin de l'alimentation de feuilles.
- N'alimentez pas ensemble un nombre de feuilles supérieur à la capacité de coupe indiquée.
- En cas d'alimentation d'un trop grand nombre de feuilles à la fois, le destructeur peut boucher. En cas de bouchage, faites glisser le commutateur dans la position « REV » (<C>) (marche arrière) afin de déboucher les feuilles et les laisser ressortir.

Notice d'utilisation des Rexel Prostyle, Style+ et Style

F

par l'ouverture de coupe. Si les feuilles restent toujours bloquées après la marche arrière, mettez l'appareil hors tension et arrachez les feuilles à la main. Recommencez ensuite l'alimentation en mettant un autre grand nombre de feuilles à la fois et en introduisant d'abord l'extrémité non découpée.

AVERTISSEMENT :

Ne faites pas fonctionner l'appareil sans arrêt pendant plus de 3 minutes. En cas de surchauffe du moteur, le dispositif de sécurité thermique se met automatiquement en marche. Dans ce cas-là, n'utilisez pas l'appareil pendant 30 minutes. Après le refroidissement du dispositif de sécurité thermique, vous pouvez réutiliser le destructeur en toute sécurité.

Vidage de la corbeille amovible (fig 4)

Videz la corbeille dès que les déchets sont visibles par la fenêtre de contrôle de remplissage, située sur le côté de la corbeille.

1. Retirez la corbeille (complètement).
2. Videz la corbeille dans un sac à poubelle.
3. Remettez la corbeille dans le destructeur en veillant à bien l'enfoncer.

AVERTISSEMENT :

- Cet appareil n'est pas un jouet. Gardez-le hors de portée des enfants et des animaux domestiques.
- Réservé à un usage intérieur.
- N'introduisez jamais les doigts dans l'ouverture de coupe du destructeur.
- Éloignez immédiatement l'appareil à vos cheveux, votre cravate ou votre manche ne prend accidentellement dans l'appareil.
- L'appareil ne fonctionne que lorsque la corbeille est bien enfoncée dans le destructeur.
- Videz la corbeille quand elle est pleine pour assurer le bon fonctionnement du destructeur.
- Avec une corbeille pleine peut entraîner un blocage de papier dans les couteaux et une hausse du niveau sonore de l'appareil.
- Ne touchez pas les déchets dans la corbeille (par exemple avec les pieds).

Spécifications techniques

Modèle	Rexel Prostyle	Rexel Style+ (VST14C)	Rexel Style NSS11C)
Type de coupe	Coupe croisée	Coupe croisée	Coupe croisée
Largeur des particules	4 x 25 mm	4 x 25 mm	4 x 30 mm
Capacité de destruction (en une fois)	11 feuilles (80 gsm)	7 feuilles (80 gsm)	5 feuilles (80 gsm)
Ouverture de coupe	230 mm	230 mm	230 mm
Dimensions de l'appareil	430 x 232 x 410 mm	378 x 209 x 360 mm	340 x 185 x 323 mm
Tension/Fréquence nominale	220-240 V-50 Hz	220-240 V-50 Hz	220-240 V-50 Hz
Intensité nominale	2 A	1,3 A	0,8 A

Si le destructeur ne démarre pas, effectuez les vérifications suivantes :

1. L'appareil est-il bien branché ?
2. Le commutateur est-il en mode « ON/AUTO » ?
3. Y a-t-il bouchage ?
4. Le moteur a-t-il surchauffé ?
5. La corbeille est-elle bien enfoncée dans le destructeur ?

En cas de bouchage du papier, veuillez suivre les instructions suivantes :

1. Vérifiez si la corbeille est trop pleine. Elle doit être vidée régulièrement pour éviter le blocage de papier dans les couteaux.
2. Faites glisser le commutateur dans la position « REV » (<C>) (marche arrière) pour faire ressortir le papier.
3. Si le papier ne ressort pas lorsque le destructeur est en mode marche arrière, faites basculer lentement le commutateur vers les positions « REV » (<C>) et « ON/AUTO ». Veillez à ne pas le faire trop rapidement pour ne pas risquer d'endommager le destructeur.

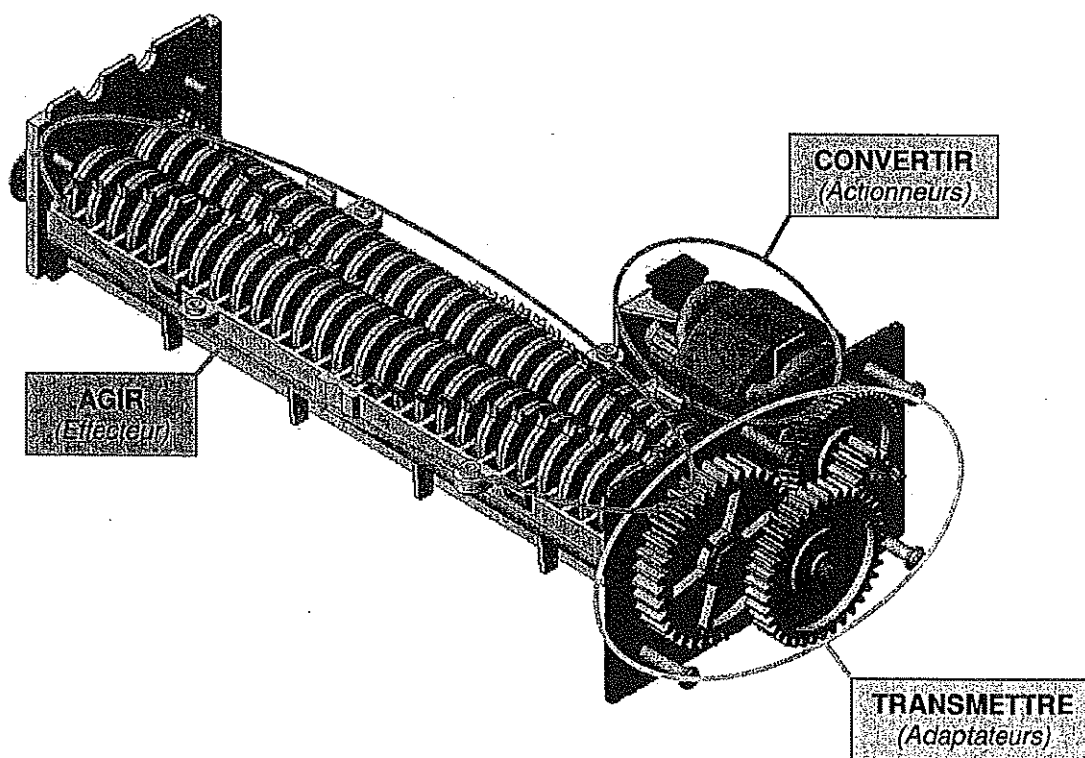
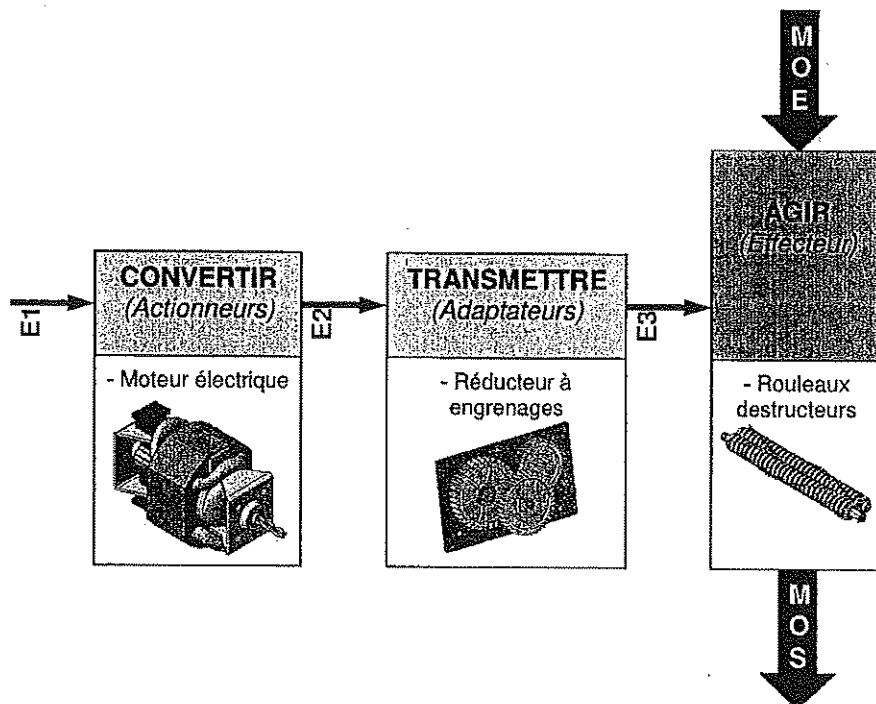
4. ATTENTION - N'essayez jamais de déboucher l'ouverture de coupe en utilisant un objet quelconque qui n'est pas prévu à cet effet (couteau, coupe-papier, etc.) - ce modèle étant alimenté sur secteur, vous risquez alors de vous infliger des blessures graves.

Cet appareil n'est pas un jouet. Gardez-le hors de portée des enfants et des animaux domestiques. En cas de surchauffe du moteur, le dispositif de sécurité thermique se met automatiquement en marche. Dans ce cas-là, n'utilisez pas l'appareil pendant 30 minutes. Après le refroidissement du dispositif de sécurité thermique, vous pouvez réutiliser le destructeur en toute sécurité.

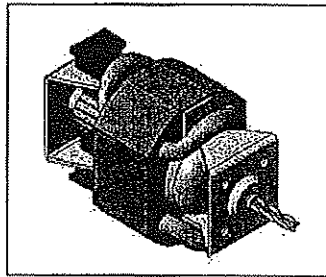
Garantie

Ce produit est garanti pendant 24 mois à partir de la date d'achat. En cas de problèmes, renvoyez l'appareil à votre fournisseur. Cela ne compromet aucunement vos droits légaux.

Chaîne de transmission de puissance :

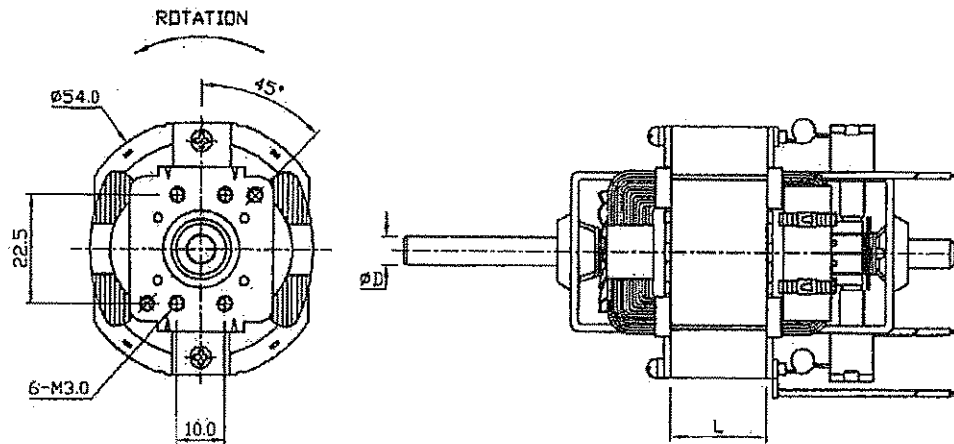


Moteur électrique « Universel » série 54 :



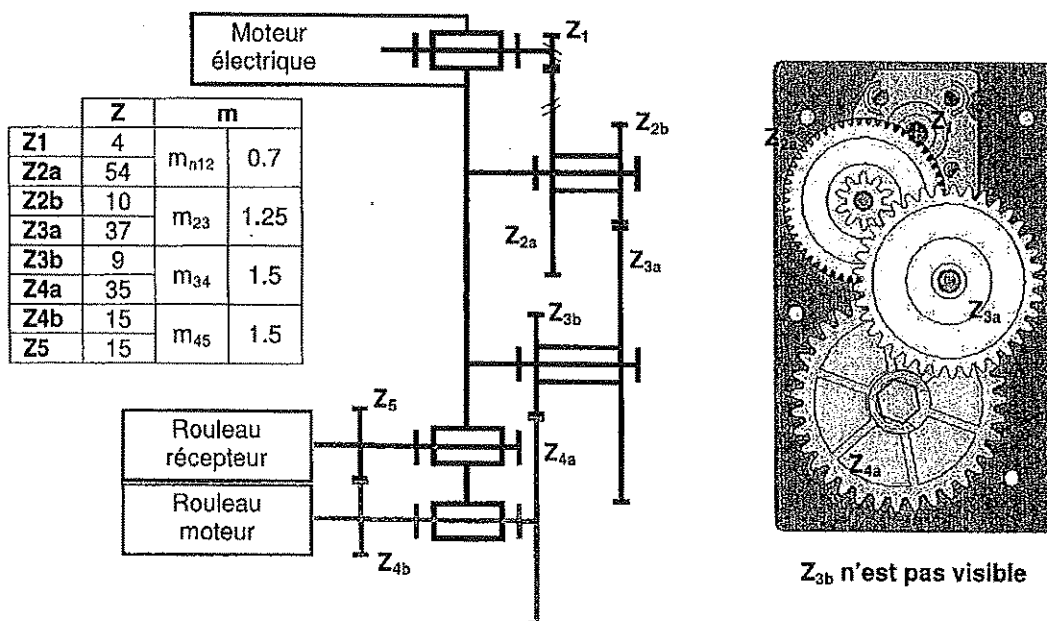
Caractéristiques moteur universel série 54 :

Tension d'alimentation : 230 V
Fréquence : 50 Hz
Intensité nominale : 0.8 A
Vitesse de rotation à vide : 25 000 tr/min
Puissance : 150 W

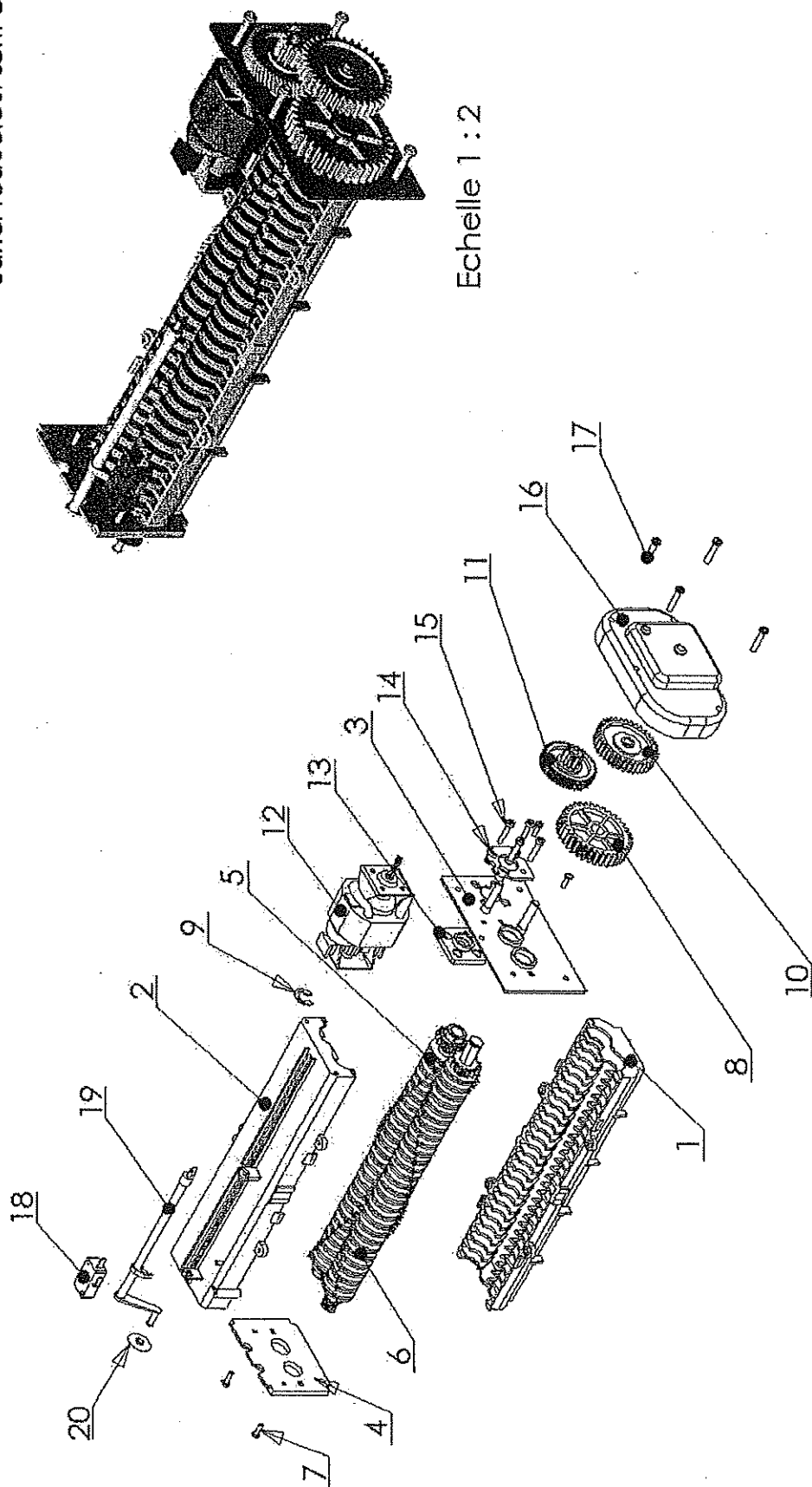


L = 12mm ~ 40mm D = 4.5 ~ 6.35mm Output Condition: Lead-wire, Terminal, Multi-speeds, Custom made Shaft

Schéma cinématique du réducteur :



Le carter supérieur et le
carter réducteur sont cachés



Destructeur de
documents

Chaîne de transmission
de puissance

Technologie Services DT9

Format : A3

Echelle 1 : 3

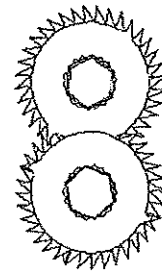
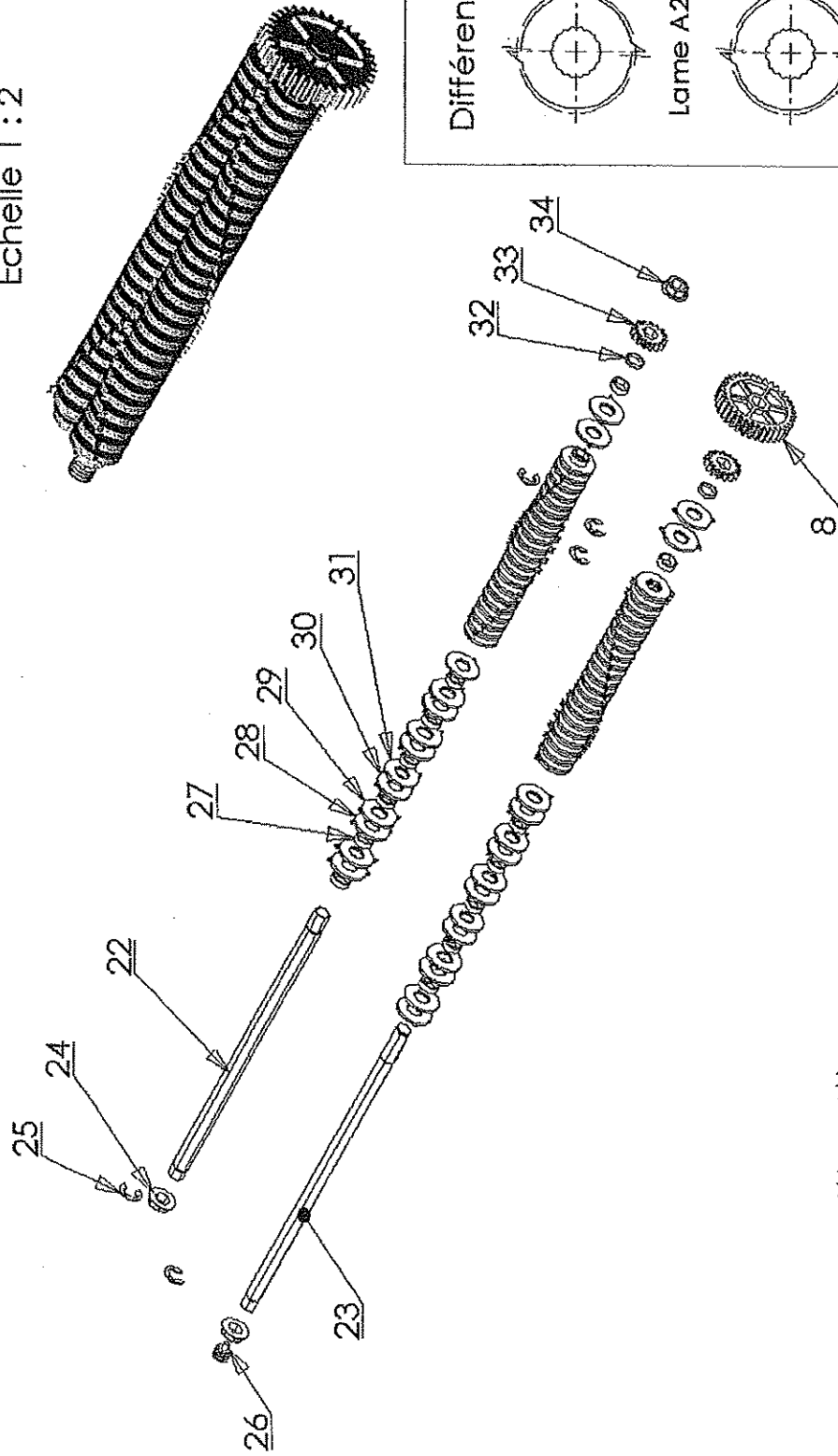
Dessiné par :

Le

Nomenclature :

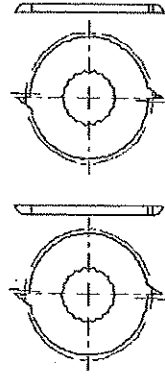
21	1	Ressort	Non représenté
20	1	Disque	
19	1	Axe de contact	
18	1	Micro rupteur	
17	4	Vis à tête cylindrique bombée large & collerette M3 x 10 – 8.8 - Z	
16	1	Carter réducteur	
15	4	Vis à tête cylindrique bombée large M3.5 x 18 – 8.8 - Z	ISO 7045
14	1	Bloc de fixation	
13	1	Bloc de fixation	
12	1	Moteur électrique universel 5424 / Pignon moteur 1	$Z_1 = 4 \text{ d} - m_n = 0.7$
11	1	Pignon intermédiaire 2	$Z_{2a} = 54 \text{ d} - m_n = 0.7$ $Z_{2b} = 10 \text{ d} - m = 1.25$
10	1	Pignon intermédiaire 3	$Z_{3a} = 37 \text{ d} - m = 1.25$ $Z_{3b} = 9 \text{ d} - m = 1.5$
9	1	Anneau élastique extérieur	
8	1	Pignon de sortie 4	$Z_4 = 35 \text{ d} - m = 1.5$
7	4	Vis à tête cylindrique bombée large M3 x 10 – 8.8 - Z	ISO 7045
6	1	Rouleau destructeur moteur	Assemblage (voir DT11)
5	1	Rouleau destructeur récepteur	Assemblage (voir DT11)
4	1	Plaque arrière	
3	1	Plaque de fixation	
2	1	Carter Supérieur	
1	1	Carter inférieur	
Rep	Nb	Désignation	Observation

Echelle 1 : 2

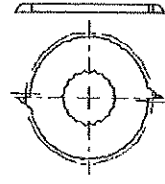


Montage des lames
Echelle 1 : 1

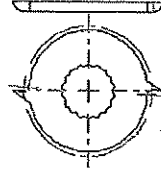
Différentes lames seules



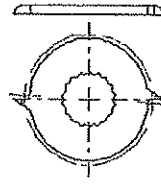
Lame A2



Lame B2



Lame A1



Lame B1

Destructeur
de documents

Format : A3

Echelle 1 : 3

Dessiné par :

Le

Rouleaux destructeurs

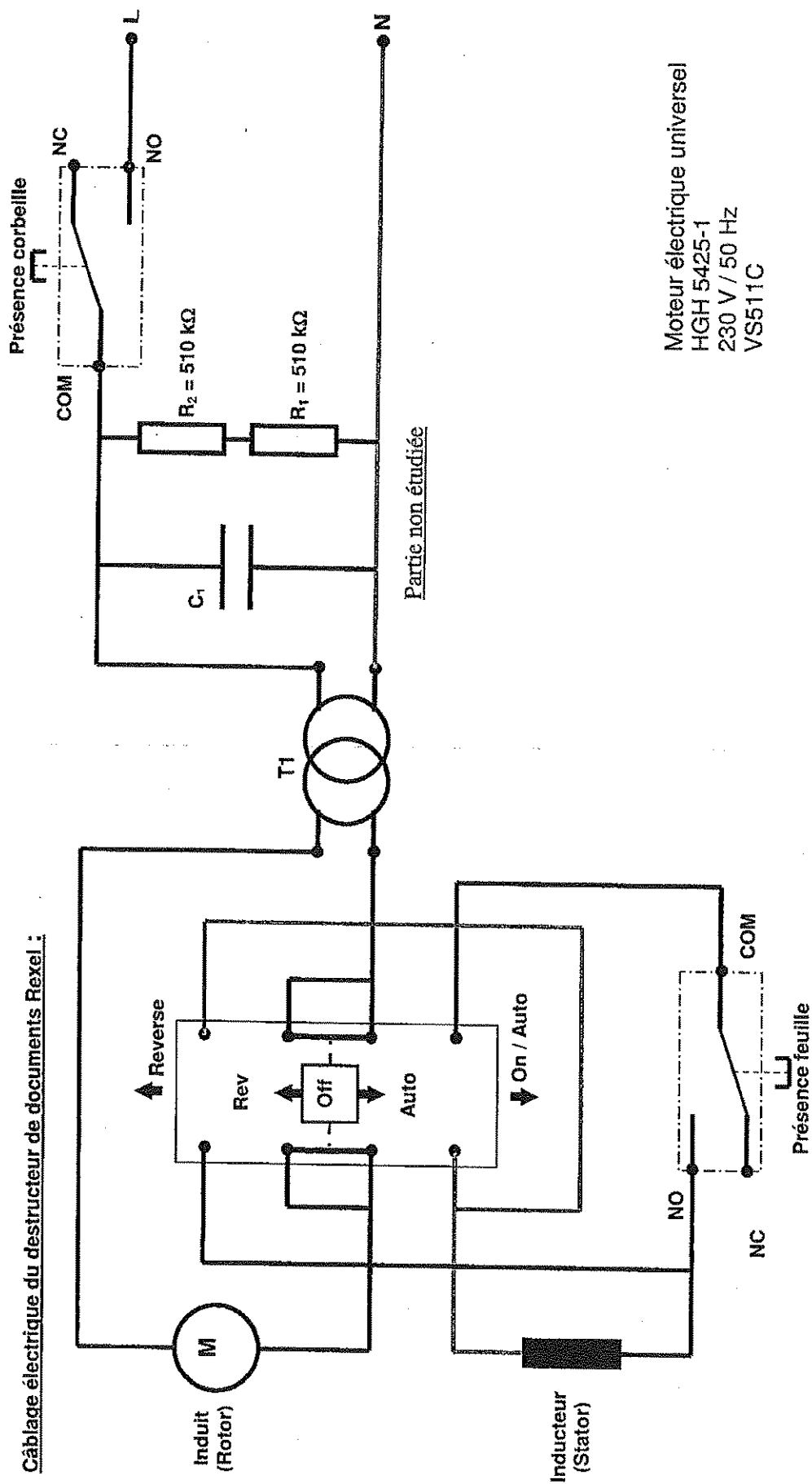
Technologie Services DT11

Nomenclature (rouleaux) :

34	1	Bague	
33	2	Engrenage cylindrique droit	Z = 15 d ; m = 1.5
32	1	Entretoise	
31	28	Lame B1	
30	28	Lame A1	
29	27	Lame B2	
28	27	Lame A2	
27	55	Entretoise	
26	1	Vis sans fin	Pas = 2 mm
25	5	Anneau élastique extérieur	
24	2	Bague	
23	1	Axe rouleau destructeur moteur	
22	1	Axe de rouleau destructeur récepteur	
Rep	Nb	Désignation	Observation

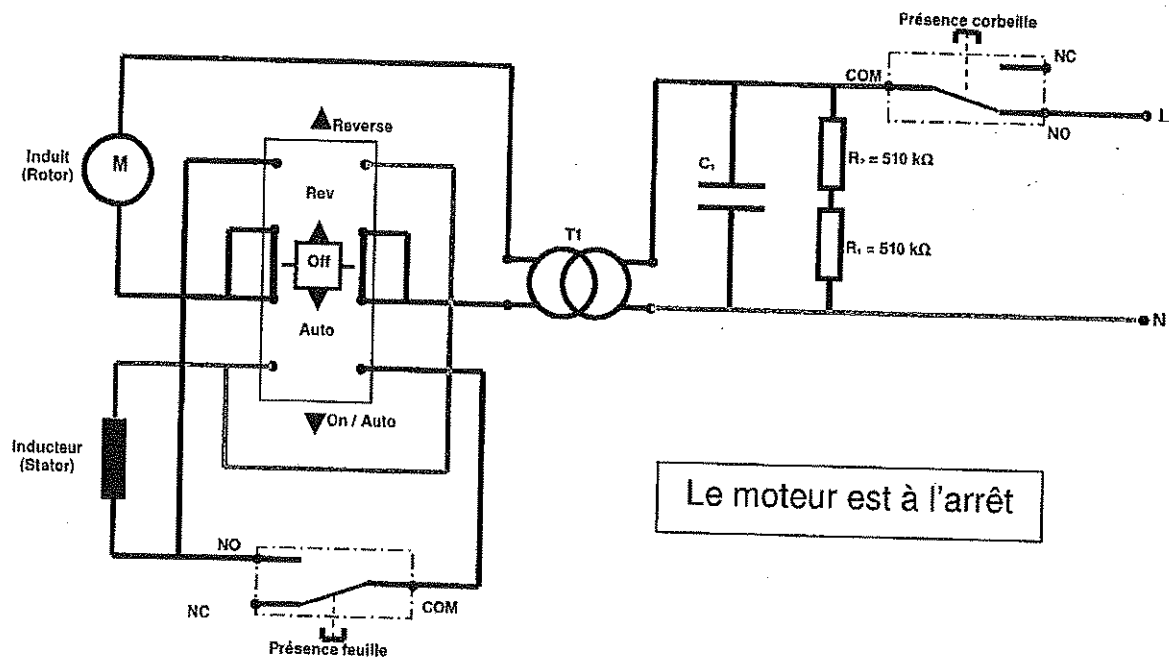
<p>Figure 1</p> <p>Le micro rupteur n'est pas enclenché.</p> <p>Le ressort est comprimé, le disque est bloqué par la vis sans fin.</p> <p>Feuille</p>	<p>Figure 2</p> <p>Contact Avo / Feuille</p>	<p>Figure 3</p> <p>Contact Avo / Micro rupteur</p> <p>Déplacement du disque</p>	<p>Figure 4</p> <p>Déplacement du obquo</p>
<p>Figure 5</p>	<p>Figure 6</p> <p>Contact Disque / Vis sans fin</p>	<p>Figure 7</p> <p>Déplacement du disque</p>	<p>Figure 8</p> <p>Il n'y a plus contact</p>
<p>Le destructeur est sur la position On/Auto. La feuille n'est pas encore en contact avec le destructeur. Le moteur ne tourne pas.</p>	<p>La feuille entre en contact avec l'axe. L'axe pivote. Le disque n'est plus en contact avec la vis.</p>	<p>L'axe entre en contact avec le micro rupteur et enclenche ainsi le moteur. Le disque, sous l'effet du ressort, se déplace en translation.</p>	<p>Le disque vient en butée.</p> <p>Lorsque le disque arrive en fin de vis, l'axe pivote. Il n'y a plus contact avec le micro rupteur. Le moteur s'arrête.</p>

Câblage électrique du destructeur de documents Rexel :

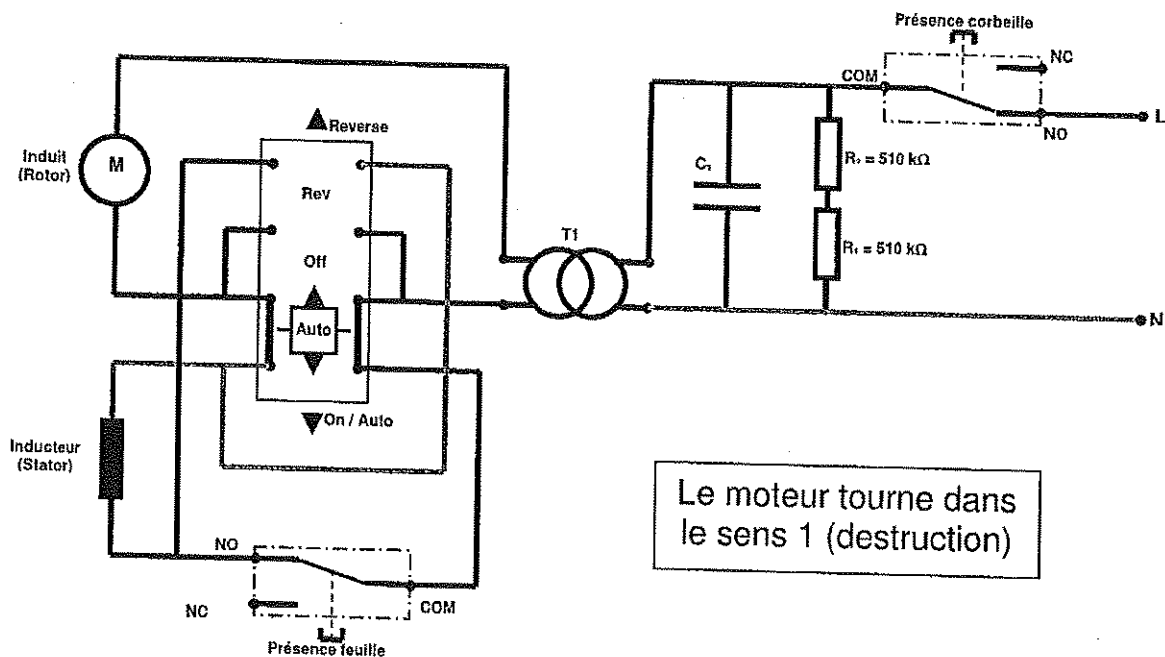


Moteur électrique universel
HGH 5425-1
230 V / 50 Hz
VS511C

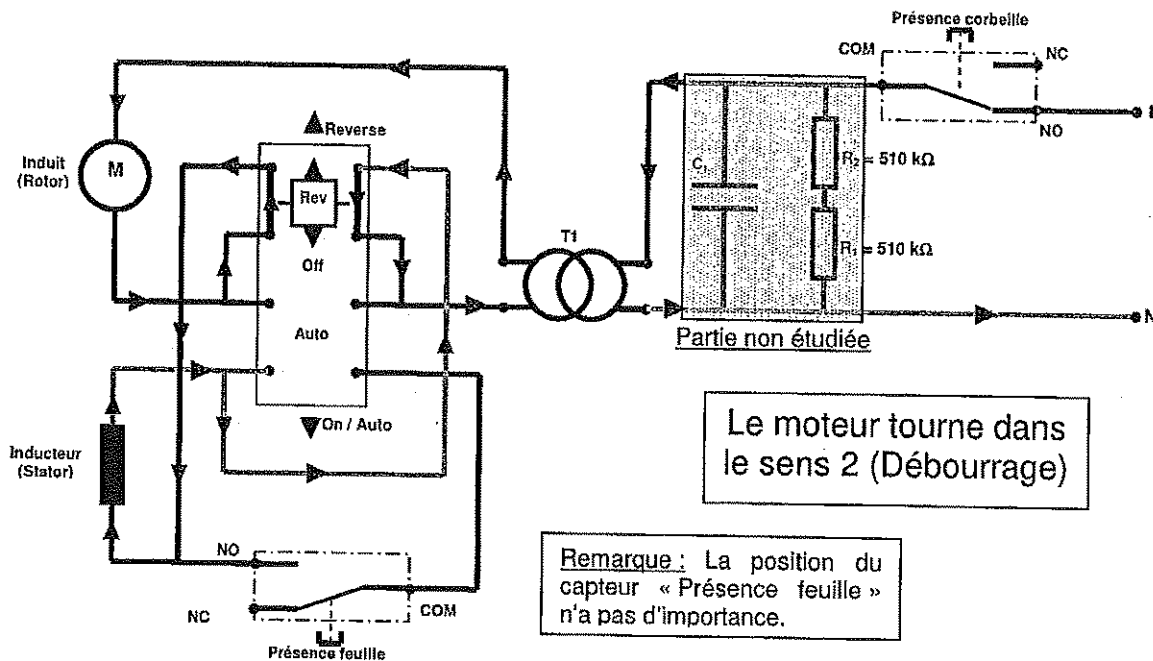
Câblage électrique du destructeur de documents Rexel : Position OFF & corbeille présente



Câblage électrique du destructeur de documents Rexel : Position ON/Auto, corbeille présente & Présence feuille



Câblage électrique du destructeur de documents Rexel : Position REV & corbeille présente



Extrait de la norme DIN32757

La norme de sécurité DIN 32757 classe les documents à détruire en 5 niveaux selon leurs contenus et assigne pour chacun un degré de destruction ne permettant aucune identification, ni aucune reconstruction. Le niveau de sécurité d'un destructeur correspond au niveau de confidentialité recherché dans la destruction du document. Plus le document est découpé finement, plus le niveau de sécurité est élevé, et plus la confidentialité des documents détruits est conservée.

- La norme DIN 32757 de niveau 1 pour les documents généraux
La classe DIN 1 regroupe les destructeurs de documents dits « coupe droite » (ou « coupe fibre ») qui découpe les documents en bandes de 12 mm de largeur maximum. Ce type de coupe convient aux documents généraux devant être rendus illisibles après écoulément du délai de conservation.
- DIN niveau 2 pour les documents internes
Au niveau de sécurité 2, nous recourons à la fois des destructeurs « coupe droite » et « coupe croisée ». Les destructeurs « coupe droite » de niveau 2 doivent découper les documents en bandes, dont la largeur est inférieure ou égale à 5 mm. Les destructeurs « coupe croisée », qui découpent les documents dans le sens de la longueur et dans le sens de la largeur, doivent réaliser des particules de moins de 800 mm². Ce genre de découpe convient aux documents internes devant être rendus illisibles.
- DIN niveau 3 pour les documents confidentiels
Pour être classés en niveau de sécurité 3 en coupe fibres, la taille des bandes doit être inférieure ou égale à 2 mm de largeur, et d'une surface inférieure ou égale à 594 mm². En coupe croisée, la particule doit avoir une largeur inférieure ou égale à 4 mm, et une longueur inférieure ou égale à 80 mm ; soit une surface de 320 mm² ou moins. Ce type de coupe convient aux documents confidentiels, comme des données concernant des personnes.
- DIN niveau 4 pour les documents confidentiels d'une importance capitale pour l'entreprise
Seuls des destructeurs de documents de type « coupe croisée » composent cette classe. Ils réduisent les documents en particules de 2 mm x 15 mm ou moins, pour une surface maximum de 30 mm² par particule. Les documents éliminés de cette manière sont des documents secrets.
- Pour la plus haute classe de la norme DIN 32757, la classe de sécurité 5, les particules doivent être de 0,8 mm x 13 mm ou moins, et d'une surface inférieure ou égale à 10 mm². Ce type de coupe convient aux documents classés ultra-secrets, qui requièrent une protection extrême.



CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C –SESSION 2017 -

CONCOURS INTERNE Epreuve écrite obligatoire

NOTE ADMINISTRATIVE

Date de l'épreuve : 28 juin 2017
Durée de l'épreuve : 3 heures
Coefficient : 3

Ce sujet comporte :

- ➡ Un énoncé : page 1
- ➡ Une documentation : pages 2 à 19

Le (la) candidat(e) est invité(e) à vérifier qu'il (elle) est en possession des pages 1 à 19.

IMPORTANT

« Afin de préserver l'anonymat des copies, il est rappelé qu'aucun signe distinctif ne doit apparaître sur la copie. Il est également vivement recommandé, sous peine d'annulation de l'épreuve concernée, de ne pas apposer sa signature, ni d'inscrire son nom, son grade ou tout autre mention personnalisée. Le nom du candidat ne doit figurer qu'à l'emplacement réservé à cet effet »

Concours interne TSEEAC

Note administrative

SUJET :

En poste auprès du cabinet de la direction du SEAC PF, vous rédigerez en vous référant aux documents joints, une note administrative pour le directeur, de 4 pages maximum, relative à la politique de sécurité contre les risques de cyber attaques affectant les compagnies aériennes. Vous présenterez l'importance de la menace ainsi que quelques mesures pratiques pouvant être mises en place pour y faire face.

DOCUMENTS JOINTS :

Document N°1 : L'Agence européenne de sécurité aérienne alerte contre le risque de cyber-attaque
Page 2 08-10-2015 <https://www.lesechos.fr>

Document N°2 : Deux hackers récompensés par une compagnie aérienne
Page 3 17-07-2015 <https://www.lemonde.fr>

Document N°3 : L'aviation subit 1000 cyber attaques par mois
Pages 4 à 6 11-07-2016 <http://www.euractiv.fr>

Document N°4 : Pirater le système de contrôle d'un avion, c'est possible selon l'Agence européenne de la sécurité aérienne
Pages 7 à 8 08-10-2015 <http://www.usinenouvelle.com>

Document N°5 : Aviation : les menaces de cyber attaques prises très au sérieux
Pages 9 à 10 16-10-2015 <https://www.franceinter.fr>

Document N°6 : Organisation de l'aviation civile internationale – Résolutions adoptées (extrait)
Pages 11 à 12 6-10-2016 <https://www.icao.int>

Document N°7 : Avis du Comité économique et social européen sur la «Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil»
Pages 13 à 17 23-07-2011 <http://eur-lex.europa.eu>

Document N°8 : Le saviez vous ?
Pages 18 à 19 17-04-2015 <http://actu.dalloz-etudiant.fr/>

Document N°1 :

L'Agence européenne de sécurité aérienne alerte contre le risque de cyber-attaque

BRUNO TREVIDIC | Le 08/10/15 à 12H10

Le directeur de l'AESA, Patrick Ky, affirme que le piratage informatique d'un avion en vol représente une réelle menace pour la sécurité du transport aérien.

Oui, le piratage informatique d'un avion est possible et oui, la cybercriminalité représente bien une véritable menace pour le transport aérien. Cette fois, ce n'est pas un « hacker » mégalomane qui le dit, mais le patron de l'Agence européenne de sécurité aérienne, Patrick Ky. Lors d'une rencontre avec l'association des journalistes de la presse aéronautique et spatiale (AJPAE), ce jeudi matin à Paris, le directeur exécutif de l'AESA a confirmé les craintes que l'on pouvait nourrir dans ce domaine. « *Croire que le transport aérien est à l'abri de ce genre de menace revient à se voiler la face, a-t-il affirmé. C'est un sujet sérieux auquel nous devons nous attaquer* ».

Le système de messages Acars piraté en moins de 5 mn

A l'appui de ses craintes, Patrick Ky a raconté comment un expert en piratage informatique employé par l'AESA était parvenu à pénétrer « *en quelques minutes* » dans le système informatique d'un avion au sol. « *J'ai fait appel à un hacker qui a la particularité d'avoir également une licence de pilote commercial, a-t-il expliqué. En moins de 5 minutes, il est parvenu à rentrer dans le réseau Acars, le système de messagerie des compagnies aériennes [qui permet d'envoyer des messages automatiques réguliers de l'avion vers le sol, sur le bon fonctionnement des systèmes critiques de l'avion NDLR]. Et il ne lui a fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait. Mais, je vous laisse juger si le risque est faible ou élevé.* »

Des failles dans le système

L'an dernier, un groupe de travail mandaté par l'Organisation de l'aviation civile internationale (OACI) avait pourtant estimé que le risque d'une cyber-attaque sur un avion en vol était très faible. Le système informatique de contrôle de l'avion est en effet théoriquement totalement séparé des autres systèmes informatiques de bord non-critiques, comme celui des communications ou des divertissements de bord. Mais les possibilités d'interconnexion ou des failles dans la muraille, existent apparemment, à en juger par l'expérience de l'AESA.

« *Demain, avec la mise en place de Sesar [le futur système européen de contrôle du trafic aérien NDLR] et la possibilité pour le contrôle du trafic aérien de donner directement des instructions au système de contrôle de l'avion, ce risque va être multiplié* », souligne Patrick Ky. D'où la volonté de son directeur de s'attaquer au sujet. « *Nous devons commencer par mettre en place une structure chargée d'alerter les compagnies aériennes sur les cyberattaques* », indique-t-il. A plus long terme, l'AESA, qui a déjà la responsabilité de la certification technique des aéronefs en Europe, pourrait également se charger de certifier les équipements contre le risque des cyber-attaques.

Document N°2 :

Deux hackers récompensés par une compagnie aérienne

United Airlines encourage les experts en sécurité informatique à débusquer les failles de son système en les récompensant de « miles ». Une première pour une compagnie aérienne.

Le Monde.fr | 17.07.2015 | Par Morgane Tual

Un million de « miles » chacun : c'est la récompense qu'a accordée la compagnie aérienne américaine United Airlines à deux hackers qui ont découvert des failles de sécurité dans son système informatique.

L'entreprise avait lancé en mai une opération appelant les experts en sécurité informatique à rechercher des failles. « Si vous pensez que vous avez découvert un bug de sécurité à même d'affecter nos sites, nos applications et/ou nos portails, faites-le nous savoir, peut-on lire sur le site de la compagnie. Si ce que vous nous montrez correspond à ce que nous cherchons, nous serons heureux de vous récompenser pour votre temps et vos efforts. »

Deux hackers, dont l'Américain Jordan WIENS, à la tête d'une start-up spécialisée, entre autres, en sécurité informatique, ont ainsi obtenu une récompense de « miles », des points de fidélité convertibles en voyages, correspondant à une valeur de plusieurs dizaines de vols domestiques.

(« Wow ! United a vraiment payé ! J'ai eu un million de miles pour ma participation au "bug Bounty". Très cool. »)

Les deux hackers n'ont toutefois pas été autorisés à dévoiler la nature des failles découvertes.

Face book récompense aussi

Ce type de programme, appelé bug Bounty (« prime de bug »), est très répandu dans le milieu des nouvelles technologies. Face book, Google et Microsoft y ont par exemple recours, pour repérer des problèmes avant que des hackers malveillants ne les exploitent. Mais c'est la première fois qu'une compagnie aérienne s'empare de ce système.

United Airlines a plusieurs fois souffert de problèmes informatiques. En 2011, elle avait dû immobiliser tous ses avions à cause d'une « panne informatique », selon un porte-parole, qui avait paralysé les systèmes de réservation et rendu impossible l'embarquement. En juin, un problème informatique avait également cloué au sol ses avions aux Etats-Unis pendant près d'une heure.

Le spectre de l'avion piraté

En avril, un chercheur en sécurité informatique, Chris Roberts, qui se trouvait dans un avion de la compagnie, avait publié un tweet facétieux sur sa capacité à pirater l'appareil. Il avait été accueilli à sa descente par le FBI, qui l'avait interrogé avant de lui confisquer son matériel. Selon un document de l'agence fédérale, il aurait affirmé avoir réussi à s'infiltrer partiellement dans les systèmes de navigation de plus d'une dizaine d'avions entre 2011 et 2014 – sans préciser les compagnies concernées. Plus grave : selon le document, Chris Roberts aurait même prétendu avoir réussi à dévier légèrement un avion en agissant sur un moteur.

Des propos dont la véracité n'a pas été établie, mais la mise en place du bug Bounty chez United Airlines constitue une réponse à ces différents problèmes de sécurité. Car en plus de permettre à la compagnie de tester la vulnérabilité de son système à peu de frais, ce programme représente aussi une opération de communication pour rassurer ses clients sur le sujet sensible de la sécurité informatique.

Morgane TUAL - Journaliste au Monde

Document N°3 :

L'aviation subit 1000 cyberattaques par mois

Par : Jorge Valero | EURACTIV.com | translated by Céline Nguyen 11 juil. 2016

L'agence européenne de sécurité des avions demande que les menaces informatiques contre les compagnies aériennes et les aéroports soient prises au sérieux.

Des avions infectés par des virus, des brèches de sécurité aux États-Unis, en Turquie, en Espagne, en Suède, et récemment en Pologne... ces dernières semaines, les problèmes informatiques se sont multipliés, entraînant retards, pertes d'informations. Et surtout une grande inquiétude des autorités publiques, des régulateurs et de l'industrie.

La crainte d'un futur dans lequel les terroristes pourraient provoquer des crashes d'avions à distance est de plus en plus palpable.

« Nous devons toujours nous préparer au pire », a confié Luc Tytgat, directeur de la gestion de la stratégie et de la sécurité à l'agence européenne de la sécurité aérienne (EASA).

Pour donner une idée de l'ampleur du défi, il a affirmé que les systèmes de l'aviation étaient sujets à 1 000 attaques par mois en moyenne.

« Nous devons prendre cela au sérieux », a-t-il averti, pressant tous les partenaires de l'EASA et les experts informatiques dans les États membres à développer « une entente commune » pour la gestion des risques et le partage des informations.

« Nous n'avons pas beaucoup de temps », a-t-il insisté.

Depuis quelques années, élaborer une stratégie commune pour contrer les cyberattaques dans ce secteur qui traverse les frontières est devenu une priorité, notamment en Europe et aux États-Unis, où se trouvent les deux géants de l'aéronautique.

Brian Moran, le vice-président aux affaires gouvernementales en Europe pour Boeing, a souligné l'« importance » d'une coopération transatlantique.

« C'est essentiel », a-t-il précisé, remarquant qu'« il y a une forte volonté de coopérer ».

Le nouveau centre informatique de l'UE

À l'échelle européenne, l'EASA va obtenir un nouveau centre de cybersécurité, a indiqué Luc Tytgat. Il contribuera à comprendre la nature des menaces, à rassembler des informations sur les attaques précédentes, identifier les failles, analyser et développer les réponses aux incidents informatiques, qu'il s'agisse de solutions de secours ou de conseils techniques.

Les efforts de l'UE reflètent les recommandations faites lors du comité consultatif de haut niveau organisé par la Federal Aviation Administration (FAA) aux États-Unis. L'objectif de ce comité est d'identifier les zones de risques et trouver un système international pour se protéger des attaques informatiques.

Les priorités de l'OACI

En accord avec l'inquiétude de plus en plus forte, la cybersécurité figurera à l'agenda de l'assemblée générale de l'OACI, organisée en septembre 2016. L'ONU a déjà qualifié cette question comme une question majeure en 2012. Or, le problème est devenu encore plus urgent entretemps.

L'OACI devrait adopter une résolution invitant les États membres à aligner leurs responsabilités de sécurité et adopter une approche flexible pour gérer l'apparition de ces nouveaux risques.

Selon Luc Tytgat, l'EASA et la FAA sont en train de penser à une position commune « en urgence » pour compléter la proposition de l'OACI.

Les pirates engagés comme conseillers en cybersécurité ont joué un rôle majeur pour mettre en avant la question.

L'expert informatique Chris Roberts avait choqué le secteur de l'aviation et les agences de sécurité en affirmant qu'il avait plusieurs fois piraté un avion transportant des passagers avec sa console de jeu, depuis son siège. Il a ajouté qu'il était en mesure de contrôler les moteurs de l'avion pendant le vol.

Suite à ces déclarations, une enquête du FBI a été ouverte et le gouvernement américain a averti le personnel des compagnies aériennes de surveiller les passagers qui tenteraient de connecter leurs ordinateurs portables aux équipements à bord.

Or, selon Hugo Teso, pirate et pilote espagnol, il n'est pas nécessaire d'avoir un ordinateur à bord.

Aujourd'hui conseiller réputé dans les compagnies aériennes, il avait stupéfié les participants à une réunion privée en 2013, en insinuant qu'il pouvait prendre le contrôle d'un avion avec son téléphone portable.

« Dans les avions modernes, il y a un grand nombre de failles, que les pirates peuvent exploiter pour accéder aux différents systèmes des machines », a-t-il averti.

Néanmoins, Brian Moran est moins alarmiste, rappelant que les avions actuels sont équipés de systèmes de protection contre ces intrusions. En revanche, il a souligné l'importance de protéger davantage les systèmes utilisés sur la terre ferme, de la maintenance à la gestion des procédures et dans le cockpit.

Les risques au sol

Les experts ont tendance à lui donner raison. Actuellement, les failles les plus importantes ont été identifiées dans les réseaux connectés aux avions qui permettent de charger ou télécharger des informations sur le vol.

L'EASA fait remarquer que les systèmes sont moins sécurisés que ceux installés dans les machines.

À l'heure actuelle, le matériel utilisé par les passagers pendant les vols, comme les connexions wi-fi et les consoles de jeux sont séparées physiquement des systèmes de sécurité à bord de l'avion. C'est pourquoi les experts ont remis en question l'affirmation de Chris Roberts d'être parvenu à contrôler les moteurs d'une machine.

Les conséquences des cyberattaques contre des systèmes au sol se sont déjà fait ressentir.

En juin 2015, une attaque avait empêché environ 1 400 passagers de prendre leur avion en paralysant les systèmes de dix avions à l'aéroport Chopin de Varsovie pendant près de cinq heures.

Les pirates ont procédé à une attaque par déni de service (DoS), une technique couramment utilisée sur internet pour surcharger un système en l'inondant de messages simultanés.

L'attaque avait pris par surprise un grand nombre d'acteurs, y compris les compagnies impliquées.

« C'est un problème industriel d'une ampleur bien plus importante et il est évident que nous devons y prêter plus attention », a assuré le PDG de la compagnie polonaise LOT, Sebastian Mikosz, lors d'une conférence de presse suivant l'incident.

« Cela peut arriver à n'importe qui, n'importe quand », a-t-il évalué.

Bien que beaucoup de compagnies aériennes et d'aéroports ont des systèmes très performants pour gérer les attaques informatiques, « ils n'ont pas adopté une approche holistique du domaine informatique ou pris en considération la menace générale pour le système d'aviation », a prévenu l'association du transport aérien international (IATA).

« Le prochain 11 septembre sera provoqué par des pirates informatiques prenant le contrôle des avions, il n'y aura pas de suicide », a prédit Gabi Siboni, le directeur du programme de cybersécurité de l'institut de recherches pour la sécurité nationale d'Israël.

Contexte

L'industrie aéronautique s'appuie largement sur les systèmes informatiques, que ce soit au sol ou dans les airs. Certains systèmes sont directement liés à la sécurité de l'avion pendant le vol, d'autres ont une importance opérationnelle. Beaucoup ont un impact direct sur le service, la réputation et la santé financière de l'industrie.

Il ne fait aucun doute que l'automatisation a fortement amélioré la sécurité et les capacités des machines en simplifiant les tâches. Cependant, le nombre de points d'entrée dans les systèmes augmente de plus en plus.

L'IATA a développé une stratégie reposant sur trois piliers pour comprendre, définir et évaluer les menaces et les risques des cyberattaques, mettre en place une réglementation adéquate et des mécanismes pour augmenter la coopération au sein de l'industrie, avec le soutien des gouvernements.

Un mécanisme de coordination a été mis en place du groupe de travail de haut niveau qui se réunit régulièrement.

Document N°4 :

Pirater le système de contrôle d'un avion, c'est possible selon l'Agence européenne de la sécurité aérienne

Olivier James Aéronautique , Aviation civile , Digital/Technos

Publié le 08/10/2015 À 16H27

Le directeur de l'Agence européenne de la sécurité aérienne (AESA) s'inquiète des failles des avions en matière de cybersécurité. Un hacker a fait la preuve concrète de cette menace auprès des experts de l'agence.

La confirmation est maintenant indiscutable. Le hacker qui avait prétendu avoir piraté un avion de ligne en mai dernier avait pourtant provoqué le scepticisme chez nombre d'experts. Le directeur de l'Agence européenne de la sécurité aérienne (AESA), Patrick Ky, a levé le doute : *"l'aviation est vulnérable à la cybercriminalité"*.

Des propos tenus jeudi 8 octobre, lors d'une rencontre avec l'Association des journalistes de la presse aéronautique et spatiale (AJPAE). Pour soutenir ses dires, Patrick Ky a expliqué en détails comment un hacker en avait fait la preuve formelle... au sein même de l'AESA !

"Nous avons organisé il y a quelques mois une cession sur la cybersécurité au sein de l'agence, raconte Patrick Ky. Un groupe de l'Organisation de l'aviation civile internationale (OACI) nous a alors assuré que le risque cybernétique était faible. Juste après cette présentation, j'ai fait intervenir un hacker, détenant également une licence de pilote d'avion commercial. En moins de cinq minutes, il est arrivé à entrer dans le réseau d'une compagnie aérienne avec un profil d'administrateur. Il s'agissait du réseau ACARS, le réseau de messageries entre l'avion et le sol".

« N'importe qui peut s'introduire n'importe où »

De quoi faire dire au hacker : *"Je vous laisse juge de savoir si le risque est faible ou élevé"*. Mais l'intrusion du pirate ne s'est pas arrêtée là. *"Au bout de deux à trois jours, ce hacker a même réussi à pénétrer dans le système de contrôle d'un avion"*, continue Patrick Ky. Et de préciser aussitôt qu'il s'agissait d'un avion au sol. Serait-il possible de réaliser la même intrusion avec un avion en vol ? Cette question provoque un sourire figé chez Patrick Ky qui préfère ne rien répondre.

Les propos du patron de l'AESA surprennent, les systèmes de contrôle et de communication de l'avion étant a priori indépendants. Sans donner de détails sur le mode opératoire du hacker, Patrick Ky assure que les failles sont maintenant prouvées. *"En matière de cybersécurité, n'importe qui peut s'introduire n'importe où, résume-t-il. Des hackers ont même réussi récemment à entrer dans le centre de commandes des drones américains"*.

Un projet de rapprochement avec les autorités américaines

La démonstration réalisée à l'AESA en toute discrétion, inquiète ces spécialistes de la sécurité aérienne. Le risque de cyber-attaque promet en effet de s'accroître dans les prochaines années avec le déploiement de Sesar, le projet de ciel unique européen qui vise à harmoniser le trafic aérien via une sorte de réseau internet fermé entre les avions et les systèmes de contrôle aérien.

La multiplication des communications entre les avions, le sol et les satellites, qui devraient favoriser une meilleure gestion du trafic aérien, pourraient aussi prêter davantage le flanc aux cyber-attaques.

"L'aviation doit arrêter de se voiler la face, assène Patrick Ky. Nous devons nous poser la question de savoir quel réseau spécifique doit être mis en place, comme on en trouve dans les secteurs de la banque ou de l'énergie. Il faut par exemple pouvoir informer le reste du réseau qu'une attaque vient de se produire".

Le patron de l'AESA milite pour un projet de rapprochement avec les autorités américaines, qui ont mis en œuvre un système d'analyse de données du trafic aérien qui permet d'identifier les risques. Il voudrait aussi impliquer les compagnies aériennes et les syndicats de pilote. En poste depuis deux ans, Patrick Ky voit la cybercriminalité comme l'un des enjeux majeurs du trafic aérien pour les années à venir.

Olivier James

Document N°5 :

vendredi 16 octobre 2015 par Margaux Duquesne

Aviation : les menaces de cyberattaques prises très au sérieux

Le piratage informatique est une réelle menace pour l'aviation. Les responsables de ce secteur restent très attentifs aux travaux de certains hackers sur la question... Enquête.

Personne ne s'était aventuré à le prononcer en ces termes auparavant : Patrick Ky, directeur exécutif de l'Agence européenne de sécurité aérienne (AESA), a déclaré, le 8 octobre dernier, devant des journalistes spécialisés dans la presse aéronautique et spatiale, que le piratage d'un avion, qu'il soit au sol ou en vol, était possible et que les cyberattaques étaient de réelles menaces pour le secteur :

Croire que le transport aérien est à l'abri de ce genre de menace revient à se voiler la face. C'est un sujet sérieux auquel nous devons nous attaquer.

Preuve à l'appui, Patrick Ky raconte avoir fait appel à un hacker, employé par l'AESA et doté d'une licence de pilote commercial, qui est parvenu à pénétrer, en quelques minutes, dans le système de messagerie des compagnies aériennes, le réseau Acars, permettant d'envoyer des messages de l'avion vers le sol. *« Et il ne lui a __fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait. Mais, je vous laisse juger si le risque est faible ou élevé, » a expliqué Patrick Ky.*

Chapeau noir et chapeau blanc

Ce n'est pas étonnant que les professionnels de l'aviation fassent appel à des hackers pour tester leurs systèmes de sécurité. En effet, il existe deux catégories de hackers : les chapeaux noirs (« *black hat* ») qui piratent des systèmes dans un but malveillant, souvent pour faire du profit (en revendant par exemple des failles de sécurité à d'autres acteurs malintentionnés), et les chapeaux blancs (« *white hat* ») qui réalisent des tests d'intrusion. Ces derniers, lorsqu'ils repèrent des failles de sécurité, alertent les entreprises ou autorités concernées pour qu'elles améliorent leur propre système de défense.

Le consultant en cybersécurité Hugo Teso en fait par exemple partie : il teste depuis des années la sécurité informatique de ce secteur et réalise des conférences sur ses recherches. En France, le responsable de la sécurité des systèmes d'information de la Direction générale de l'aviation civile (DGAC), Jean Carlioz, l'a rencontré, avec grand intérêt. Et il le prend très au sérieux :

« C'est un type jeune, très timide, qui a visiblement une grande expertise du sujet, qui ne s'interdit pas de fanfaronner mais tout est basé sur une vraie compétence, commence-t-il. Il nous avait fait une démonstration en montrant qu'en moins de 15 minutes il pouvait accéder à un système de navigation aérienne. » Jean Carlioz est conscient des risques de cyberattaque mais tempère, en expliquant qu'en contrepartie les autorités se préparent à ce risque potentiel d'attaque :

Si un gouvernement étranger ou des gens dotés de moyens considérables voulaient vraiment mettre le paquet, faire une ingénierie sociale, voler des mots de passe et faire comme font les hackers, c'est-à-dire peu à peu se rendre maître d'un système... au bout d'un moment, ils y arriveront, ce n'est qu'une question de temps, continue Jean Carlioz, de la DGAC. Sauf que pendant ce temps-là, nous évaluons le risque, on se nourrit des déclarations de personnes comme Hugo Teso, qui ont un vrai intérêt s'ils nous alertent. Constamment, nous essayons d'élever les niveaux des systèmes.

Des petits écrans... aux commandes de l'avion

Les tests d'Hugo Teso ne sont pas sans rappeler une autre expérience rapportée par un hacker, beaucoup plus controversé. En avril dernier, l'ingénieur en sécurité informatique Chris Roberts a affirmé avoir pris le contrôle, depuis l'avion, des écrans au dos des sièges-passagers, là où l'on diffuse les films pendant le vol. Il a même envoyé un tweet où il plaisante en se demandant quel message affiché : *« Mettez vos masque à oxygen »*, par exemple;

Appréhendé par le FBI, deux jours plus tard, à la sortie d'un autre vol, il a expliqué avoir également réussi, en passant par le système gérant ces écrans de divertissement, à prendre les commandes de l'avion et à le détourner de sa trajectoire initiale. Une expérience, peut-être mal retranscrite dans l'enquête du FBI, et qui aurait en fait pu être réalisée dans un laboratoire, après reconstruction en conditions réelles.

Au moment de la médiatisation de cet événement, de nombreux spécialistes ont affirmé que les systèmes de divertissement et le système qui gère les commandes d'un avion sont totalement séparés, ne permettant pas de passerelle entre l'un et l'autre. Pourtant, en théorie, cette expérience n'est pas si irréaliste, comme nous le rapporte Gerome Billois, spécialiste en cybersécurité à Solucom

« Dans l'absolu, ce n'est pas impossible : les avions aujourd'hui utilisent des réseaux informatiques qui sont censés être cloisonnés entre le réseau de loisir et le réseau de pilotage. Le problème est que même s'ils sont cloisonnés informatiquement, derrière, ils utilisent souvent physiquement les mêmes câbles. On se retrouve alors dans une situation où s'il y a des failles de sécurité, on peut potentiellement rebondir d'une zone à une autre et au final avoir accès au système de pilotage et faire dévier la course de l'avion si on envoie les bons messages. »

Cellule de crise, en cas de crash

Quand l'avion allemand de la Germanwings s'est crashé, j'étais personnellement dans la cellule de crise parce qu'[une attaque informatique] pouvait être une hypothèse, qui a tout de suite été prise en compte. Ayant accès à toutes les données, et aux boîtes noires, on a pu lever le doute sur le fait que ce n'était pas une attaque informatique.

Des menaces assez préoccupantes, ce peut paraître logique puisque dans l'informatique, comme dans bien d'autres secteurs, la sécurité n'est jamais acquise: *« La sécurité à 100%, cela n'existe pas, explique Gerôme Billois. Quelqu'un qui aurait énormément de temps, énormément de moyens, arrivera à un moment donné à trouver une faille de sécurité, que ce soit, dans un avion, dans une voiture ou dans tous les systèmes qu'on peut imaginer. »*

C'est comme dans la sécurité physique de tous les jours : vous pouvez avoir la chambre forte la plus sécurisée au monde, avec beaucoup de temps et d'argent vous allez quand même pouvoir réussir à rentrer.

Cependant, Gerome Billois relativise: *« Tout un chacun ne peut en prenant l'avion et en se branchant sur les prises USB qu'on voit de plus en plus dans les sièges des voyageurs, d'un seul coup prendre le contrôle de l'avion et le faire se crasher. Bien heureusement il y a des mécanismes de sécurité qui ont été mis en place et qui assure une sécurité normale qui répond à la majeure partie des risques. »*

Un rapport américain accablant

A l'heure actuelle, aucune communication officielle d'aucune compagnie n'a jamais admis ce genre d'incident. Il s'avère en tout cas, d'après les déclarations dans les médias des autorités de l'aviation de ces derniers mois, que ce sujet est devenu pour eux l'une de leurs priorités. La France et l'Europe ne sont pas les seuls à s'en inquiéter : en janvier dernier, le Government Accountability Office (GAO), l'organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis, publiait un rapport accablant adressé à la Federal Aviation Administration - la FAA est l'agence gouvernementale chargée des réglementations et des contrôles concernant l'aviation civile aux États-Unis-. Les 42 pages du rapport indiquent que les problèmes de cybersécurité menacent la capacité de la FAA d'assurer un fonctionnement sûr et sans interruption du système de l'espace aérien du pays.

Parmi les 17 recommandations rendues publiques (168 autres recommandations ont été publiés dans un document confidentiel non accessible au public), le GAO demande davantage de formation à ces problématiques de cybersécurité pour les employés, un renforcement des protocoles de contrôles d'accès avec l'identification et l'authentification des utilisateurs des systèmes et un chiffrement des données sensibles.

Document N°6 :

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

RÉSOLUTIONS ADOPTÉES PAR L'ASSEMBLÉE

ASSEMBLÉE – 39e SESSION

Montréal, 27 septembre – 6 octobre 2016

...

A39-19 : Cybersécurité dans l'aviation civile

L'Assemblée,

Considérant que le système mondial de l'aviation est un système éminemment complexe et intégré constitué de technologies de l'information et des communications essentielles à la sécurité et à la sûreté des vols d'aviation civile,

Notant que le secteur de l'aviation dépend de plus en plus de la disponibilité des systèmes de technologies de l'information et des communications, ainsi que de l'intégrité et de la confidentialité des données,

Consciente que la menace représentée par les cyberincidents pour l'aviation civile évolue rapidement et continuellement, que les responsables de ces menaces sont animés d'intentions malveillantes et concentrent leurs efforts sur la perturbation de la continuité des activités et le vol d'informations pour des motivations politiques, financières ou autres, et que cette menace peut facilement évoluer et porter atteinte aux systèmes critiques de l'aviation civile dans le monde entier,

Reconnaissant que tous les problèmes de cybersécurité qui compromettent la sécurité de l'aviation civile ne sont pas illégaux et/ou intentionnels, et devraient donc être traités par l'application de systèmes de gestion de la sécurité,

Réaffirmant l'importance et l'urgence de protéger les systèmes et les données des infrastructures critiques de l'aviation civile contre les cybermenaces,

Considérant la nécessité de travailler de façon collaborative en vue de l'élaboration d'un cadre mondial efficace et coordonné permettant aux parties prenantes de l'aviation civile de relever les défis en matière de cybersécurité, et de prendre des mesures à court terme pour renforcer la résistance du système mondial de l'aviation aux cybermenaces qui peuvent compromettre la sécurité de l'aviation civile,

Reconnaissant la valeur des initiatives, plans d'action, publications et autres médias conçus pour faire face aux problèmes de cybersécurité de manière collaborative et approfondie,

Rappelant les initiatives des dirigeants du Conseil international des aéroports (ACI), de la Civil Air Navigation Services Organisation (CANSO), de l'Association du transport aérien international (IATA), du Conseil international de coordination des associations d'industries aérospatiales (ICCAIA) et de l'OACI qui attestent la nécessité de travailler ensemble et d'être guidés par une vision, une stratégie et une feuille de route communes pour renforcer la protection du système mondial de l'aviation contre les cybermenaces et sa résistance à celles-ci,

Reconnaissant la nature multiforme et multidisciplinaire des défis et des solutions en matière de cybersécurité,

1. Invite les États et les parties prenantes de l'industrie à prendre les mesures suivantes pour contrer les cybermenaces auxquelles est confrontée l'aviation civile :

a) Déterminer les menaces et les risques associés aux éventuels cyberincidents contre les vols et les systèmes critiques de l'aviation civile, et les graves conséquences que peuvent entraîner de tels incidents ;

- b) Définir les responsabilités des organismes nationaux et des parties prenantes de l'industrie en ce qui concerne la cybersécurité dans l'aviation civile ;
- c) Encourager le développement d'une compréhension commune entre les États membres pour ce qui est des cybermenaces et des cyberrisques, et l'élaboration de critères communs pour établir la criticité des ressources et des systèmes qui nécessitent une protection ;
- d) Encourager la coordination des gouvernements et de l'industrie quant aux stratégies, politiques et plans relatifs à la cybersécurité dans l'aviation, ainsi que le partage d'informations pour aider à déceler les vulnérabilités critiques auxquelles il faut remédier ;
- e) Développer, à l'échelle nationale et internationale, des partenariats et des mécanismes gouvernements-industries, et jouer un rôle dans lesdits partenariats et mécanismes, afin que soient systématiquement partagées les informations sur les cybermenaces, les incidents, les tendances dans ce domaine et les efforts d'atténuation ;
- f) Sur la base d'une compréhension commune des cybermenaces et des cyberrisques, adopter une approche souple et fondée sur les risques pour la protection des systèmes critiques d'aviation grâce à la mise en œuvre de systèmes de gestion de la cybersécurité ;
- g) Encourager une solide culture générale en matière de cybersécurité dans les organismes nationaux et dans l'ensemble du secteur de l'aviation ;
- h) Déterminer les conséquences judiciaires des activités qui compromettent la sécurité de l'aviation en exploitant les cybervulnérabilités ;
- i) Promouvoir l'élaboration et la mise en œuvre de normes, stratégies et meilleures pratiques internationales relatives à la protection des systèmes critiques de technologies de l'information et des communications utilisés aux fins de l'aviation civile contre des interventions qui peuvent compromettre la sécurité de l'aviation civile ;
- j) Établir des politiques et affecter des ressources, au besoin, afin que, en ce qui concerne les systèmes d'aviation critiques : la sécurité soit intégrée à la conception des architectures de systèmes ; les systèmes soient résistants ; les méthodes de transfert de données soient sécurisées, assurant ainsi l'intégrité et la confidentialité des données ; la surveillance des systèmes et les méthodes de détection et de compte rendu d'incidents soient mises en œuvre ; des analyses techniques des cyberincidents soient réalisées ;
- k) Collaborer à l'élaboration du cadre de cybersécurité de l'OACI selon une approche horizontale, transversale et fonctionnelle qui met à contribution la navigation aérienne, la communication, la surveillance, l'exploitation technique et la navigabilité des aéronefs et d'autres disciplines pertinentes.

2. Charge le Secrétaire général :

- a) d'aider les États et l'industrie à prendre ces mesures et de leur faciliter la tâche en ce sens ;
- b) de veiller à ce que les questions de cybersécurité soient dûment examinées et coordonnées dans toutes les disciplines pertinentes de l'OACI.

...

Document N°7 :

Avis du Comité économique et social européen sur la «Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil»

COM(2010) 517 final — 2010/0273 (COD)

2011/C 218/27

Rapporteur général: M. MORGAN

Le Conseil, en date du 20 janvier 2011 a décidé, conformément à l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), de consulter le Comité économique et social européen sur la:

«Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil»

COM(2010) 517 final — 2010/0273 (COD).

Le 15 février 2011, le Bureau du Comité économique et social européen a chargé la section spécialisée «Transports, énergie, infrastructures, société de l'information» de préparer les travaux du Comité en la matière. Compte tenu de l'urgence des travaux (article 59 du règlement intérieur), le Comité économique et social européen a décidé au cours de sa 471^e session plénière des 4 et 5 mai 2011 (séance du 4 mai 2011) de nommer M. Peter MORGAN rapporteur général, et a adopté le présent avis par 173 voix pour, 1 voix contre et 7 abstentions.

1. Conclusions et recommandations

- 1.1 Le Comité accueille favorablement la communication de la Commission concernant la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information. Le Comité partage la vive préoccupation de la Commission concernant l'ampleur de la cybercriminalité en Europe et les dommages réels et potentiels que cette menace qui s'amplifie fait ou peut faire subir à l'économie et au bien-être des citoyens.
- 1.2 Le Comité déplore tout comme la Commission que seuls 17 des 27 États membres aient jusqu'à ce jour ratifié la convention du Conseil de l'Europe sur la cybercriminalité («convention sur la cybercriminalité») ⁽¹⁾. Le Comité appelle les autres États membres ⁽²⁾, à savoir la Belgique, la République tchèque, l'Irlande, la Grèce, le Luxembourg, Malte, l'Autriche, la Pologne, la Suède et le Royaume-Uni, à ratifier cette convention sur la cybercriminalité dès que possible.
- 1.3 Le Comité estime tout comme la Commission qu'une directive est nécessaire d'urgence pour actualiser les définitions des infractions liées aux attaques contre des systèmes d'information et pour accroître la coopération et la coordination en matière de justice pénale au niveau de l'UE afin d'apporter une réponse efficace à ce problème critique.
- 1.4 Vu la nécessité urgente d'une action législative qui traite spécifiquement les attaques contre les systèmes d'information, le Comité approuve la décision de la Commission de recourir à une directive, étayée par des mesures non législatives, afin de cibler cet aspect particulier de la cybercriminalité.
- 1.5 Toutefois, comme l'a demandé le CESE dans un précédent avis ⁽³⁾, il souhaiterait que la Commission poursuive, en parallèle, ses travaux visant à élaborer un corpus complet de législation européenne contre la cybercriminalité. Le Comité estime qu'un cadre global est essentiel pour la réussite de l'agenda numérique et de la stratégie Europe 2020 ⁽⁴⁾. Il convient que ce cadre traite des questions de prévention, de détection et d'éducation en sus de la répression et de la sanction.
- 1.6 Le CESE souhaite examiner en temps voulu les propositions de la Commission relatives à un cadre global d'action en vue d'aborder la question générale de la sécurité de l'internet. Si nous nous projetons dans dix ans, lorsque la plupart des citoyens utiliseront l'internet, lorsque la plupart des activités économiques et sociales dépendront de l'internet, il n'est pas concevable que nous continuions encore de nous en remettre à l'approche actuelle de l'utilisation de l'internet, qui se caractérise par la négligence et l'absence de méthode, tout particulièrement lorsque que cette activité a une valeur économique incalculable. De nombreux problèmes se présenteront, qui soulèveront d'autres défis tels que la sécurité des données à caractère personnel et relevant de la vie privée ou encore la cybercriminalité. En matière de sécurité aérienne, une

autorité centrale veille et établit des normes pour les avions, les aéroports et les activités des compagnies aériennes. Il est temps de créer une autorité semblable qui établit des normes pour des équipements terminaux sans failles (ordinateurs personnels, tablettes, téléphones), la sécurité des réseaux, la sécurité des sites internet et celle des données. La configuration physique de l'internet est un élément crucial dans la défense contre la cybercriminalité. L'UE va avoir besoin d'une instance de régulation avec des pouvoirs sur l'internet.

- 1.7 La directive à l'examen vise essentiellement à définir le crime et établir les peines afférentes. Le CESE demande qu'elle vise en parallèle à la prévention grâce à de meilleures mesures de sécurité. Il y a lieu que les fabricants d'équipement satisfont à des normes pour la fourniture de produits sans failles de sécurité. Il n'est pas acceptable que la sécurité de ces produits et, par conséquent, celle des réseaux dépendent de la bonne volonté de leur propriétaire. Il y a lieu d'envisager la mise en place d'un dispositif d'identification électronique dans toute l'Europe, qu'il convient cependant de concevoir avec soin afin d'éviter d'enfreindre la vie privée; il y a lieu de commencer à exploiter pleinement les possibilités de la version six du protocole internet (IPv6) en matière de sécurité; il y a lieu que l'apprentissage des citoyens de leur propre cybersécurité, y compris celle de leurs données, soit une composante essentielle de tout programme d'études dans le domaine des compétences numériques. À cet égard, il serait utile que la Commission se réfère aux avis antérieurs du Comité qui traitent de ces questions (5).
- 1.8 Le Comité estime que la directive proposée couvre comme il se doit les attaques contre les systèmes d'information au moyen de botnets (6), y compris les attaques par déni de service (7). Le Comité estime également que la directive aidera les autorités à poursuivre les actes de cybercriminalité qui tentent d'exploiter l'interconnectivité internationale des réseaux, de même que les personnes qui essaient de se cacher derrière l'anonymat susceptible d'être offert par les outils sophistiqués inhérents à ce type de criminalité.
- 1.9 Le Comité se félicite également de la liste des infractions pénales couvertes par la directive, en particulier de l'inclusion de l'«interception illégale», et de la précision apportée aux «Outils utilisés pour commettre les infractions».
- 1.10 Toutefois, eu égard à l'importance de la confiance et de la sécurité dans l'économie numérique, et au coût annuel énorme de la cybercriminalité (8), le Comité estime que la sévérité des sanctions prévues dans la directive devrait refléter la gravité du crime et aussi revêtir un effet dissuasif réel pour les criminels. La directive proposée prévoit des peines minimales de deux à cinq ans d'emprisonnement (cinq en cas de circonstances aggravantes). Le CESE prévoit une gradation des peines liée à la gravité du crime.
- 1.11 Le CESE est d'avis qu'il convient aujourd'hui de saisir l'occasion d'envoyer un message fort aux criminels et aux citoyens qui souhaitent être rassurés en prévoyant des peines plus sévères. Par exemple, les attaques à grande échelle contre les systèmes d'information sont passibles de sanctions allant jusqu'à dix années d'emprisonnement au Royaume-Uni (9), tandis que l'Estonie a renforcé les sanctions contre l'utilisation d'attaques à grande échelle à des fins terroristes, lesquelles sont punissables d'une peine maximale de 25 ans d'emprisonnement (10).
- 1.12 Le Comité se félicite de la proposition de la Commission d'appuyer la directive par des mesures non législatives visant à promouvoir la poursuite des actions coordonnées au niveau de l'UE et une application plus efficace du droit. Le CESE entend également souligner la nécessité d'élargir cette coordination de sorte qu'elle comprenne une étroite coopération avec tous les pays de l'AELE et l'OTAN.
- 1.13 Le Comité est très favorable aux programmes de formation et aux recommandations concernant les meilleures pratiques proposées pour accroître l'efficacité des points de contact 24/7 existants pour les services chargés de l'application de la loi.
- 1.14 En sus des mesures non législatives mentionnées dans la proposition, le Comité plaide auprès de la Commission notamment pour qu'elle oriente des ressources de recherche et développement vers le développement de systèmes de détection et de réaction précoces pour les attaques visant les systèmes d'information. Les technologies les plus avancées d'informatique en nuage («cloud computing») (11) et de grilles informatiques («grid computing») (12) recèlent la capacité de protéger davantage l'Europe contre de nombreuses menaces.
- 1.15 Le Comité suggère que l'ENISA mette sur pied un programme ciblé de développement des compétences qui viserait à renforcer l'industrie européenne de la sécurité des TIC en allant au-delà des seuls aspects répressifs (13).
- 1.16 En vue de renforcer les défenses européennes contre les cyberattaques, le Comité entend réitérer l'importance que revêtent le développement d'un partenariat public privé européen pour la résilience (EP3R) et son intégration avec les travaux de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et du groupe des CERT gouvernementaux européens (EGC).

- 1.17 Il convient de stimuler en Europe une industrie forte de la sécurité de l'information pour faire jeu égal avec les compétences d'une industrie nord-américaine qui dispose de très grands moyens financiers (14). Les investissements dans la R&D et l'éducation en matière de cybersécurité doivent être accrus de manière considérable.
- 1.18 Le Comité prend note qu'au titre des protocoles au traité, le Royaume-Uni, l'Irlande et le Danemark ne sont pas tenus d'appliquer la directive proposée. Sans préjudice de ces exemptions, le Comité appelle ces États membres à coopérer dans toute la mesure du possible avec les dispositions de la directive en vue d'empêcher que des criminels n'exploitent les lacunes des politiques à l'échelle de l'Union.

2. Introduction

- 2.1 Aujourd'hui, l'Europe dépend fortement des systèmes d'information pour la création de richesse et pour sa qualité de vie. Il est important que notre dépendance croissante aille de pair avec une sophistication de plus en plus poussée des mesures de sécurité et une réglementation stricte afin de protéger les systèmes d'information des attaques.
- 2.2 Internet est la plateforme de base de la société numérique. La lutte contre les menaces à la sécurité des systèmes d'information revêt une importance cruciale pour le développement de la société numérique et l'économie numérique. Internet soutient la plupart des infrastructures d'information critiques d'Europe, qui constituent les plateformes d'information et de communication sous-jacentes à l'offre de biens et services essentiels. Les attaques contre les systèmes d'information, qu'il s'agisse des systèmes officiels, des systèmes financiers, des services sociaux et des infrastructures vitales telles que la fourniture d'énergie, d'eau, de transports, de services de santé et de première urgence, constituent désormais un problème majeur.
- 2.3 L'architecture d'Internet se fonde sur l'interconnexion de millions d'ordinateurs dont les fonctions de traitement, de communication et de contrôle se répartissent à travers le monde. Cette architecture décentralisée est la clé de la stabilité et de la résilience d'Internet: elle permet une récupération rapide des flux de trafic lorsqu'un problème se produit. Cependant, des cyberattaques de grande envergure peuvent être lancées de ses nœuds de bordure, comme dans le cas des réseaux de machines zombies, par n'importe quel voyou, à qui il suffit d'être mal intentionné et de disposer de quelques connaissances de base.
- 2.4 L'évolution des technologies de l'information aggrave encore le problème en facilitant la production et la distribution des outils («maliciels» (15) et «botnets»), tout en offrant l'anonymat aux délinquants et en éparpillant la responsabilité entre divers pays. La difficulté d'engager des poursuites qui en résulte permet ainsi à la criminalité organisée de réaliser des profits considérables à peu de risques.
- 2.5 Selon une étude réalisée en 2009 (16) et présentée au Forum économique international, le coût global de la cybercriminalité est d'un milliard de dollars et il augmente rapidement. Et un rapport (17) récemment mené par les autorités britanniques l'estime à 27 millions de livres rien que pour le Royaume-Uni. Le coût élevé de la cybercriminalité justifie l'adoption de mesures sévères, leur application stricte et des sanctions lourdes pour les délinquants.
- 2.6 Comme l'explique le document de travail des services de la Commission qui accompagne la proposition de directive (18), la criminalité organisée et les régimes hostiles exploitent le potentiel destructeur des attaques contre les systèmes d'information dans l'Union européenne. Les attaques menées par ces «réseaux zombies» peuvent s'avérer très dangereuses pour l'ensemble du pays touché et peuvent également être exploitées, par des terroristes notamment, afin de faire peser une pression politique sur un État.
- 2.7 L'attaque menée en Estonie en avril-mai 2007 a mis ce problème en exergue. À cette occasion, d'importantes parties des infrastructures d'information critiques officielles et du secteur privé se sont retrouvées inopérantes pendant plusieurs jours suite à des attaques à grande échelle menées contre elles. Au total, ces attaques ont coûté de 19 à 28 millions EUR et ont eu des retombées politiques majeures. Des attaques destructives similaires ont également été lancées contre la Lituanie et la Géorgie.
- 2.8 Les réseaux mondiaux de communication requièrent un degré d'interconnexion transfrontalière élevé. Il est vital que les 27 États membres mènent une action collective et uniforme afin de lutter contre la cybercriminalité, et en particulier les attaques contre les systèmes d'information. Du fait de cette interdépendance internationale, il incombe à l'UE de définir une politique intégrée visant à protéger les systèmes d'information des attaques et à sanctionner les auteurs de ces dernières.
- 2.9 Dans son avis de 2007 sur «Une stratégie pour une société de l'information sûre» (19), le Comité souhaitait l'adoption d'une législation européenne complète sur la lutte contre la cybercriminalité. Outre les attaques

contre les systèmes d'information, ce cadre global concernerait la cyberdélinquance financière, les contenus illégaux sur Internet, les collectes/stockages/transferts de preuves électroniques, et il détaillerait davantage les règles de compétence.

- 2.10 Le Comité reconnaît que l'élaboration d'un cadre global est une mission très complexe, rendue encore plus difficile par l'absence de consensus politique (20) et par les problèmes nés de la divergence significative entre les différents États membres en ce qui concerne l'admissibilité des preuves électroniques devant les tribunaux. Cependant, ce cadre global permettrait d'exploiter au maximum les avantages des instruments législatifs et autres qui visent à lutter contre le large spectre de problèmes liés à la cybercriminalité. Il traiterait également des mesures pénales et dans le même temps améliorerait la coopération en matière de répression au sein de l'Union européenne. Le Comité invite la Commission à poursuivre ses travaux en vue de définir un cadre juridique global en matière de lutte contre la cybercriminalité.
- 2.11 La lutte contre la cybercriminalité requiert des compétences spécifiques. L'avis du Comité sur la proposition de règlement concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) (21) souligne l'importance de la formation pour les autorités chargées de l'application de la loi. Le Comité se réjouit de constater que la Commission progresse dans la création de la plate-forme de formation en matière de cybercriminalité incluant les services répressifs et le secteur privé telle que proposée dans le document COM(2007) 267 (22).
- 2.12 Est partie prenante de la cybersécurité de l'UE tout citoyen dont la vie peut dépendre de ces services vitaux. Ces mêmes citoyens sont responsables de la protection, au mieux de leurs possibilités, de leur connexion à Internet contre des attaques. Une plus grande responsabilité encore incombe aux fournisseurs de services et de technologies de TIC qui pourvoient les systèmes d'information.
- 2.13 Une information suffisante et adéquate de toutes les parties intéressées constitue un élément crucial de la cybersécurité. Il est donc fondamental pour l'Europe de disposer d'un grand nombre d'experts qualifiés dans le domaine de la cybersécurité.
- 2.14 Il convient de stimuler en Europe une industrie forte de la sécurité de l'information pour faire jeu égal avec les compétences d'une industrie nord-américaine qui dispose de très grands moyens financiers (23). Il convient d'augmenter sensiblement les investissements dans la recherche et le développement et l'éducation en matière de cybersécurité.

3. Contenu essentiel de la proposition de directive

- 3.1 La présente proposition a pour objet de remplacer la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information (24). Ainsi qu'il ressort de ses considérants, la décision-cadre visait à renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information. Elle créait ainsi une législation européenne permettant de poursuivre des infractions telles que l'accès illicite à un système d'information, l'atteinte à l'intégrité d'un système et l'atteinte à l'intégrité des données, ainsi que des dispositions spécifiques relatives à la responsabilité des personnes morales, la compétence juridictionnelle et les échanges d'informations. Les États membres étaient tenus de prendre les mesures nécessaires à sa transposition le 16 mars 2007 au plus tard.
- 3.2 Le 14 juillet 2008, la Commission a publié un rapport sur la transposition de la décision-cadre (25). Le rapport concluait que «des récentes attaques perpétrées en Europe depuis l'adoption de la décision-cadre ont souligné l'émergence de [plusieurs] menaces, que constituent notamment les attaques massives commises simultanément contre plusieurs systèmes d'information et l'utilisation accrue des "botnets" à des fins criminelles.» Ce type d'attaques n'était pas au centre des attentions lors de l'adoption de la décision-cadre.
- 3.3 La présente proposition tient compte des nouvelles méthodes adoptées pour commettre des infractions informatiques, notamment le recours aux «botnets» ou «réseaux zombies» (26). Il est difficile de repérer les coupables car les ordinateurs qui composent le réseau zombie et lancent l'attaque peuvent se trouver ailleurs.
- 3.4 Les attaques par réseaux zombies sont souvent réalisées à grande échelle, c'est-à-dire avec des outils qui atteignent un grand nombre de systèmes d'information (ordinateurs) ou en causant un préjudice considérable, eu égard aux services de réseau perturbés, au coût financier, aux pertes de données à caractère personnel, etc. Les dommages causés par de telles attaques à grande échelle ont des incidences majeures sur le fonctionnement de la cible en tant que telle et/ou elles affectent son environnement de travail. Par conséquent,

un «grand réseau zombie» aurait la capacité de causer un grave préjudice. Il n'est pas aisé de définir la taille des réseaux zombies mais les plus grands qui ont été observés auraient, d'après les estimations, entre 40 000 et 100 000 connexions (c'est-à-dire ordinateurs contaminés) par période de 24 heures (27).

- 3.5 La décision-cadre comporte plusieurs failles, imputables à l'évolution de la taille et du nombre d'infractions (cyberattaques). En effet, elle ne rapproche les législations que sur un nombre limité d'infractions et ne permet pas de faire face à la menace potentielle que les attaques à grande échelle représentent pour la société. Elle ne tient pas non plus suffisamment compte de la gravité des infractions et ne prévoit pas de sanctions à leur mesure.
- 3.6 La directive a pour objet de rapprocher les règles pénales appliquées par les États membres pour réprimer les attaques contre les systèmes d'information et de renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres.
- 3.7 Les attaques contre les systèmes d'information, en particulier celles qui pourraient émaner du milieu de la criminalité organisée, constituent une menace croissante, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information des infrastructures critiques des États membres et de l'Union suscite de plus en plus l'inquiétude. Cette situation risque de compromettre la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union européenne.
- 3.8 On constate une tendance à la perpétration d'attaques à grande échelle de plus en plus dangereuses et régulières contre des systèmes d'information critiques pour les États ou certaines fonctions du secteur public ou privé. Parallèlement, des outils de plus en plus sophistiqués sont mis au point, lesquels peuvent être utilisés par des criminels pour lancer des cyberattaques de divers types.
- 3.9 Il importe d'arrêter des définitions communes dans ce domaine, notamment pour les systèmes d'information et les données informatiques, de manière à garantir l'application cohérente de la présente directive dans tous les États membres.
- 3.10 Il convient d'adopter une position commune sur les éléments constitutifs des infractions pénales en créant les infractions communes d'accès illicite à un système d'information, d'atteinte à l'intégrité d'un système, d'atteinte à l'intégrité des données et d'interception illégale de données.
- 3.11 Il conviendrait que les États membres prévoient des sanctions pour réprimer les attaques contre les systèmes d'information. Les sanctions ainsi fixées devraient être effectives, proportionnées et dissuasives.
- 3.12 Tout en abrogeant la décision-cadre 2005/222/JAI, la directive reprendra ses dispositions actuelles et inclura les nouveaux éléments décrits ci-après.

- (a) elle incrimine la production, la vente, l'acquisition en vue de l'utilisation, l'importation, la distribution ou la mise à disposition par d'autres moyens de dispositifs/outils utilisés pour commettre les infractions;
- (b) elle prévoit des circonstances aggravantes:

- la grande ampleur des attaques – les réseaux zombies ou dispositifs similaires seraient incriminés en créant de nouvelles circonstances aggravantes, en ce sens que la mise en place d'un réseau zombie ou d'un dispositif similaire constituerait un facteur aggravant lors de la commission des infractions énumérées dans la décision-cadre existante;
- lorsque les attaques sont commises en dissimulant l'identité réelle de l'auteur et en causant un préjudice au titulaire légitime de l'identité;

- (c) elle crée l'infraction d'«interception illégale»;
- (d) elle introduit des mesures pour améliorer la coopération européenne en matière de justice pénale en consolidant la structure existante des points de contact 24/7 (28);
- (e) elle répond au besoin d'établir des statistiques sur les infractions informatiques, notamment les infractions énumérées dans la décision-cadre existante et la nouvelle infraction d'«interception illégale»;
- (f) Dans les définitions des infractions pénales énumérées aux articles 3, 4, 5 (accès illégal à des systèmes d'information, atteinte à l'intégrité d'un système et atteinte à l'intégrité des données), la directive contient une disposition qui permet de n'incriminer que les «cas qui ne sont pas sans gravité» lors de la transposition de la directive en droit national.

Bruxelles, le 4 mai 2011. Le président du Comité économique et social européen : Staffan NILSSON

Document N°8 :

Le saviez-vous ?

17 avril 2015

Cybercriminalité : quelles sanctions pour l'intrusion dans les systèmes informatiques ?

En l'absence de définition en droit interne et européen, les Nations unies ont tenté de dessiner les contours de la cybercriminalité en déclarant qu'il s'agit de « toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique ». Dans son rapport de 2011, l'Observatoire national de la délinquance et des réponses pénales (ONDRP) regroupe les infractions en deux catégories :

- les infractions où l'informatique est le moyen du délit. Sont alors visées toutes les formes d'infractions classiques facilitées par l'informatique : l'escroquerie, la pédopornographie, les atteintes à la vie privée, la propagande terroriste, etc. ;
- les infractions où l'informatique est l'objet du délit. Il s'agit des atteintes à la sécurité des systèmes et des réseaux ou des données informatiques (piratage, intrusion sur les sites, vols de données, etc.), comme notamment la cyber attaque dont a été victime TV5 Monde.

Les sanctions pour les infractions de cette dernière catégorie sont prévues aux articles 323-1 à 323-7 du Code pénal, issus de la loi n°88-19 du 5 janvier 1988 et complétés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Ainsi, aux termes de 323-1 du Code pénal, « [l]e fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ». La sanction est portée à 3 ans d'emprisonnement et 45 000 euros d'amende lorsqu'il y a en plus, soit suppression ou modification de données contenues dans le système, soit une altération du fonctionnement de ce système (C. pén., art. 323-1, al. 2).

S'agissant du fait d'entraver ou de fausser le fonctionnement d'un système, la peine encourue est de 5 ans d'emprisonnement et de 75 000 euros d'amende (C. pén., art. 323-2).

Outre ces sanctions, l'article 323-5 du Code pénal prévoit des peines complémentaires telles que la privation des droits civiques, civils et familiaux, l'interdiction d'exercer une fonction publique ou d'exercer l'activité professionnelle dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

Sources : *Rép. pén.*, Fr. Chopin, V° « Cybercriminalité » ; Féral-Schuhl, *Cyberdroit 2011/2012*, 6^e éd., Dalloz, coll. « Praxis », 2010.

http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Référence

■ Code pénal

Article 323-1

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »

Article 323-2

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

Article 323-5

« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »



CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C – SESSION 2017

CONCOURS INTERNE/EXTERNE

Epreuve écrite facultative

ALLEMAND

Date de l'épreuve : 28 juin 2017

Durée de l'épreuve : 1 heure

Coefficient : Bonus (interne et externe)

Ce sujet comporte :

- ➡ Page de garde : 1
- ➡ Texte : page 1
- ➡ Questions : page 2

Joseph Leschinsky - auch Lesche genannt - will aus den USA in seine Heimat zurückkehren und in die Sprache, die er noch immer liebt. [...]

"Lesche", sagte ich zu mir, "am besten, du gehst in die Emigrantencafeteria in der 86. Straße, Ecke Broadway. Dort ist zwar nichts los, aber draußen auf der Straße ist auch nichts los. Seit Jahren spazierst du jeden Abend den Broadway auf und ab.

Was für ein Leben ist das?!"

"Lesche", sagte ich zu mir, "du hast zwei Romane veröffentlicht, die keine Erfolge waren. Sie sind inzwischen vergessen. Amerika hat dein Genie nie verstanden. Du hast keine Freunde, wenigstens keine wirklichen. Du hast den amerikanischen Traum nie geträumt und kannst mit ihm nichts anfangen. Autos bedeuten dir nichts.

Und ein Haus im Grünen mit Kind und Kegel auch nicht. Die Jagd nach dem Dollar hast du nie mitgemacht. Du hast vom Erfolg als Schriftsteller geträumt, aber der ist ausgeblieben."

Die Emigrantencafeteria war hell erleuchtet. Die Emigranten saßen wie üblich dicht am Fenster. Jeden Abend saßen sie hier. Auch für sie hatte sich nichts geändert, nur dass sie älter geworden waren. Lesche grüßte die Emigranten und steuerte dann auf den Tisch zu, an dem Singer (1) saß. Lesche holte sich am Tresen einen Käsekuchen und eine Tasse des wässrigen amerikanischen Kaffees.

"Ich habe gehört, dass Sie Amerika verlassen wollen", sagte Singer. "Es heißt, dass Sie nach Deutschland zurückkehren."

"Ja", sagte Lesche. "Ich fliege übermorgen nach London, weil ein englischer Verlag (2) ein Buch von mir herausbringt. Dann geht es weiter nach München. Aber ich weiß nicht, ob ich in München bleibe. Vielleicht fahre ich weiter nach Berlin."

"Wenn ich an Ihrer Stelle wäre", sagte Singer, "dann würde ich mich für Berlin entscheiden. "

"Warum?" fragte Lesche.

"In Berlin können Sie schnell Kontakte mit literarischen Kreisen (3) knüpfen." Er erzählte Lesche dann von den vielen Künstlerkneipen in Berlin, wo sich Verleger und Schriftsteller trafen, und überzeugte ihn schließlich, nach Berlin zu ziehen.

"Und Sie wollen in Deutschland bleiben?"

"Ich habe genug von Amerika. Ich habe mir die Sache gründlich überlegt", sagte Lesche. "Ich bin deutscher Schriftsteller und brauche die deutsche Sprache. Ich muss sie hören, immer und überall. Außerdem ist Deutschland heute ein demokratisches Land. Der Krieg ist längst vorüber, und inzwischen ist eine neue Generation herangewachsen."

Edgar Hilsenrath: *Berlin ... Endstation*, dtv, 2006

- (1) Singer ist auch ein deutscher Emigrant
- (2) der Verlag: la maison d'edition

Beantworten Sie folgende Fragen

**1. Warum möchte Leschinsky wieder nach Deutschland zurückgehen?
Nennen Sie 5 verschiedene Gründe und schreiben Sie dann eine
Zusammenfassung. (8 points)**

**2. Text A: Schreiben Sie nur die richtigen Aussagen ab und begründen
Sie sie mit einem Zitat aus dem Text!**
(6 points)

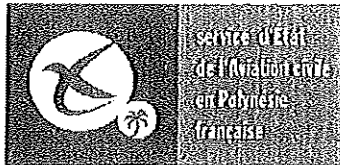
Beispiel: O. In Berlin kann man viele Künstler treffen.

Zitat: "Er erzählte Lesche dann von den vielen Künstlerkneipen in Berlin. "
(Zeilen 28-29)

- 1. Leschinskys zwei erste Romane sind den Lesern in Erinnerung geblieben.
- 2. Die Emigranten treffen sich regelmäßig.
- 3. Sein aktuelles Leben gefällt Leschinsky nicht.
- 4. Geld war wichtig für Leschinsky.
- 5. Leschinsky will in Amerika bleiben.
- 6. In England erscheint bald ein Buch von Leschinsky.

3. Übersetzen Sie den zweiten Paragraphen

("Die Emigrantencafeteria ... ") bis ("... Kaffees ") ins Französische.
(6 points)



CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C – Session 2017 -

CONCOURS EXTERNE/INTERNE

Epreuve Ecrite facultative

CONNAISSANCES AERONAUTIQUES

Date de l'épreuve : 27 juin 2017
Durée de l'épreuve : 1 heure
Coefficient : 1 (bonus)

CALCULATRICE INTERDITE

Ce sujet comporte :

- une page de garde
- une page d'instructions aux candidats,
- quatre pages de QCM (20 questions),
- une grille-réponse

INSTRUCTIONS AUX CANDIDATS

Epreuve facultative de connaissances aéronautiques

Vérifiez que votre sujet comporte :

- 1 page de garde
- 1 page d'instructions aux candidats
- 4 pages de QCM (20 questions)
- 1 grille-réponse

Instructions pour l'utilisation de la grille-réponse :

- Lisez attentivement chaque question, il n'y a qu'une seule bonne réponse possible par question ;
- L'épreuve est notée sur 20, chaque bonne réponse rapporte 1 point (1 point par question) ;
- Une mauvaise réponse ou une absence de réponse est notée 0.
- Complétez la grille-réponse à l'aide d'un stylo à bille ou feutre à pointe fine noir ou bleu. L'usage du crayon papier est interdit ;
- Il ne vous est délivré qu'une seule grille réponse, retranscrivez vos réponses après vous être relu(e) soigneusement ;
- Sur la grille-réponse, tracez une croix dans la case correspondant à votre choix ;
- Si vous désirez modifier une réponse, noircissez complètement la case et tracez une croix au nouvel emplacement. Exemple :

Questions \ Réponses	2
A	
B	
C	
D	

Identification :

N'oubliez pas de reporter votre numéro d'inscription de table sur la grille-réponse.

CONCOURS TSEEAC CEAPF EXTERNE ET INTERNE

SESSION 2017

EPREUVE FACULTATIVE

CONNAISSANCES AERONAUTIQUES

- 1) Un monomoteur fait un trajet en VFR, de 25 NM sans vent, avec une vitesse de croisière constante de 100 kts. Quelle est la durée du vol ?
 - a) 25 minutes
 - b) 8 minutes
 - c) 15 minutes
 - d) 12 minutes

- 2) Sur une carte au 1/500.000, quelle distance sur le terrain est représentée par 3cm ?
 - a) 5,5 NM
 - b) 15 km
 - c) 7.500 m
 - d) 90 hm

- 3) Qu'est-ce qu'un gisement ?
 - a) Route magnétique à suivre pour rejoindre une station
 - b) Angle entre la direction du nord magnétique et la route à suivre
 - c) Angle formé par le nord magnétique et le nord vrai
 - d) Angle relevé entre l'axe longitudinal de l'avion et la station émettrice

- 4) Trouvez l'affirmation qui est fausse au sujet du transpondeur.
 - a) C'est un émetteur-récepteur (transmetteur/répondeur) placé à bord de l'avion
 - b) En liaison avec l'altimètre, le transpondeur communique aussi l'altitude au contrôle
 - c) Le code est communiqué à l'équipage, par le contrôleur
 - d) En cas de détresse, le code affiché est 7600

- 5) Que signifie l'abréviation SCT ?
 - a) Nuages épars
 - b) Couvert
 - c) Nuages fragmentés
 - d) Peu de nuage

- 6) Le TAF est une prévision d'aérodrome. Il est divisé en combien de parties ?
 - a) 3 parties

- b) 2 parties
 - c) 5 parties
 - d) 4 parties
- 7) La foudre est générée par quels nuages ?
- a) Nimbostratus
 - b) Cumulus
 - c) Cumulonimbus
 - d) Stratocumulus
- 8) Quelles sont les caractéristiques d'une masse d'air polaire ?
- a) Froide et humide
 - b) Chaude et humide
 - c) Froide et sèche
 - d) Chaude et sèche
- 9) L'aire de manœuvre est la partie d'un aérodrome à utiliser pour :
- a) Les décollages et les atterrissages y compris les voies de circulation
 - b) La circulation des aéronefs à la surface y compris les aires de trafic
 - c) La translation des hélicoptères sur l'aire de trafic
 - d) L'avitaillement
- 10) Un pilote VFR arrive de jour aux abords d'une CTR de classe D, à destination de l'aérodrome contrôlé qui s'y trouve. La visibilité dans la CTR est de 3500 m.
- a) Il peut intégrer la circulation d'aérodrome sans restriction
 - b) Il doit se dérouter
 - c) Il doit obtenir une clairance VFR spécial avant de pénétrer dans la CTR
 - d) Il peut intégrer la circulation d'aérodrome s'il a visuel de la piste en service
- 11) Le service d'information de vol est rendu :
- a) Aux seuls vols VFR
 - b) Aux seuls vols IFR
 - c) Aux seuls vols VFR en espace aérien contrôlé et aux IFR
 - d) A tous les vols dont la présence est connue
- 12) En France métropolitaine en espace aérien non contrôlé, les vols IFR :
- a) sont interdits
 - b) sont soumis à contact radio
 - c) doivent évoluer en VMC
 - d) sont dispensés de FPL
- 13) La prévention du péril animalier sur un aérodrome doté d'un organisme de la circulation aérienne est placée sous la responsabilité :

- a) de la collectivité locale concernée
- b) du gestionnaire de l'aérodrome
- c) des compagnies aériennes basées
- d) de l'Etat

14) L'altitude d'un aérodrome publiée sur la carte VAC est de 252 pieds.

Le QFE du jour est de 1017 hPa. Quelle est la valeur du QNH sur cet aérodrome ?

- a) 1013 hPa
- b) 1008 hPa
- c) 1026 hPa
- d) 1017 hPa

15) Une piste est orientée 053°/233° par rapport au Nord Vrai. La déclinaison magnétique est de 3°W.

Quels sont les QFU de cette piste?

- a) 06/24
- b) 05/23
- c) 050°/230°
- d) 056°/236°

16) Les conditions météorologiques de vol à vue de jour en espace aérien contrôlé de classe D ou E au-dessus du niveau 100 sont les suivantes :

- a) Distance par rapport aux nuages : horizontalement ≥ 1500 m verticalement ≥ 300 m - visibilité en vol ≥ 5 km
- b) Distance par rapport aux nuages : horizontalement ≥ 1500 m, verticalement ≥ 300 m - visibilité en vol ≥ 8 km minimum
- c) Hors nuages - visibilité en vol : 8 km
- d) Hors nuage en vue de la surface - visibilité en vol : 5 km

17) Le bord de fuite est :

- a) Le bord avant de l'aile
- b) Le saumon de l'aile
- c) Le bord arrière de l'aile
- d) Le côté préférentiel pour l'évacuation de l'avion

18) Quel avantage présente un train d'atterrissage rétractable, en comparaison à un train fixe ?

- a) De faciliter l'entretien
- b) D'améliorer la portance en croisière
- c) De réduire la traînée en vol
- d) D'être plus léger

19) La finesse est le rapport :

- a) Poussée sur poids

- b) Portance sur traînée
- c) Poids sur poussée
- d) Traînée sur portance

20) Qu'indique le variomètre ?

- a) La vitesse verticale
- b) La pente de la trajectoire
- c) La vitesse air
- d) Les variations de l'inclinaison

CONCOURS DE L'AVIATION CIVILE TSEEAC/CEAPF

- SESSION 2017 -

Epreuve facultative de : CONNAISSANCES AERONAUTIQUES

N° de table du candidat :

GRILLE REPONSE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A																				
B																				
C																				
D																				



CONCOURS DE L'AVIATION CIVILE T.S.E.E.A.C – Session 2017 -

CONCOURS EXTERNE/INTERNE

Epreuve Ecrite Obligatoire

MATHEMATIQUES

Date de l'épreuve : 27 juin 2017
Durée de l'épreuve : 2 heures
Coefficient : 3 (concours externe)
2 (concours interne)

CALCULATRICE INTERDITE

Ce sujet comporte :

- Les consignes : page 1-2,
- sujet Maths : page 3 à page 11,
- grilles de réponse : page 12 et page 13 à remettre à la fin de l'épreuve.

MATHEMATIQUES

Cette épreuve comporte 25 questions.

Tout dispositif électronique est INTERDIT (en particulier l'usage de la calculatrice).

Chaque question comporte au plus deux réponses exactes.

A chaque question numérotée de 1 à 25, correspond sur la feuille " Grille de réponses " une ligne de cases qui porte le même numéro.

Chaque ligne comporte 5 cases A, B, C, D, E.

Pour chaque ligne numérotée de 1 à 15, vous vous trouverez en face de 4 possibilités :

- 1) Soit vous décidez de ne pas traiter cette question : la ligne correspondante doit rester vierge.
- 2) Soit vous jugez que la question comporte une seule bonne réponse : vous devez faire une croix sur l'une des cases A, B, C, D.
- 3) Soit vous jugez que la question comporte deux réponses exactes : vous devez faire une croix sur deux des cases A, B, C, D et deux seulement.
- 4) Soit vous jugez qu'aucune des réponses proposées A, B, C, D n'est bonne : vous devez alors faire une croix sur E.

Chaque question rapporte 1 point.

Attention : Toute réponse fausse entraîne une pénalité dans la note ; une réponse fausse = -0,5.

Questions liées :

1 à 3

4 à 8

9 à 11

12 à 19

20 à 23

Les autres questions sont indépendantes.

Partie I

Soient deux nombres complexes $Z_1 = 2 - 2i\sqrt{3}$ et Z_2 dont le module est $\frac{1}{2}$ et un argument est $\frac{-5\pi}{6}$.

QUESTION 1 :

Un argument de Z_1 est :

- A) $\frac{2\pi}{3}$.
- B) $\frac{-\pi}{3}$.
- C) $\frac{5\pi}{3}$.
- D) $\frac{7\pi}{6}$.

QUESTION 2 :

Le module de $Z_1 Z_2$ est égal à :

- A) 20.
- B) 6.
- C) 8.
- D) 10.

QUESTION 3 :

Un argument de $Z_1 Z_2$ est égal à :

- A) $\frac{5\pi}{2}$.
- B) $\frac{5\pi}{6}$.
- C) $\frac{5\pi}{8}$.
- D) $\frac{-5\pi}{6}$.

Partie II

Nous rappelons que $e^{ix} = \cos(x) + i\sin(x)$, où e est la base du logarithme népérien, x est un nombre réel et i est le nombre complexe défini par $i^2 = -1$.

QUESTION 4 :

Si x est différent de $2k\pi$, où k est un entier, la partie imaginaire du nombre complexe $1 + e^{ix} + e^{2ix}$ est égale à :

- A) $\sin(x) + \sin(2x)$.
- B) $\frac{\sin(x) \cdot \cos(\frac{3x}{2})}{\sin(\frac{x}{2})}$.
- C) $\frac{\sin(x) \cdot \sin(\frac{3x}{2})}{\sin(\frac{x}{2})}$.
- D) $\sin(x) + \sin^2(x)$.

QUESTION 5 :

Si x est différent de $2k\pi$, où k est un entier, la partie réelle du nombre complexe $1 + e^{ix} + e^{2ix}$ est égale à :

- A) $1 + \cos(x) + 2\cos(x)$.
- B) $1 + \cos(x) + \cos^2(x)$.
- C) $1 + \cos(x) + \cos(2x)$.
- D) $\frac{\cos(x) \cdot \sin(\frac{3x}{2})}{\sin(\frac{x}{2})}$.

Soient deux nombres complexes $z_1 = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$ et $z_2 = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$.

QUESTION 6 :

La somme $1 + z_1 + z_1^2$ est égale à :

- A) $1 + \frac{\sqrt{3}}{2} - \frac{i}{2}$.
- B) 0.
- C) $\frac{3}{2} - i\frac{\sqrt{3}}{2}$.
- D) $\frac{1+i\sqrt{3}}{2}$.

QUESTION 7 :

Une écriture exponentielle de $z_1^3 \times z_2$ est :

- A) $e^{\frac{i\pi}{15}}$.
- B) $e^{\frac{2i\pi}{5}}$.
- C) $e^{\frac{-3i\pi}{5}}$.
- D) $e^{\frac{2i\pi}{15}}$.

QUESTION 8 : Le nombre complexe z_1^4 est :

- A) $\frac{1+i\sqrt{3}}{2}$.
- B) $\frac{1-i\sqrt{3}}{2}$.
- C) $\frac{i+\sqrt{3}}{2}$.
- D) $\frac{-1+i\sqrt{3}}{2}$.

Partie III

La durée de vie, en heures, d'une ampoule est une variable aléatoire T qui suit la loi exponentielle de paramètre 0,0008.

QUESTION 9 :

La probabilité que l'ampoule tombe en panne avant 2000 heures est égale à :

- A) $1 - e^{-0,16}$.
- B) $1 - e^{1,6}$.
- C) $1 - e^{0,16}$.
- D) $1 - e^{-1,6}$.

QUESTION 10 :

La probabilité que l'ampoule fonctionne sans panne au moins 3000 heures est égale à :

- A) $1 - e^{-2,4}$.
- B) $1 - e^{-24}$.
- C) e^{-24} .
- D) $e^{-2,4}$.

QUESTION 11 :

La probabilité que l'ampoule tombe en panne entre la 2000 ième heure et la 4000 ième heure est égale à :

- A) $e^{-1,6} + e^{-3,2}$.
- B) $1 - e^{-1,6} + e^{-3,2}$.
- C) $e^{-1,6} + e^{-3,2} - 1$.
- D) $e^{-1,6} - e^{-3,2}$.

Partie IV

Soit f la fonction définie sur \mathbb{R} par $f(x) = \frac{e^{2x} - 5}{e^x + 3}$.

QUESTION 12 :

On a alors :

- A) $f(x) = \frac{e^{2x} - 5}{3}$.
- B) $f(x) = \frac{2 - 5e^{-x}}{3e^{-x} + 1}$.
- C) $f(x) = \frac{e^x - 5e^{-x}}{3e^{-x} + 1}$.
- D) $f(x) = \frac{e^x - 5e^{-x}}{e^x + 3e^{-x}}$.

QUESTION 13 :

La dérivée f' de f sur \mathbb{R} est définie par :

- A) $f'(x) = \frac{2e^{2x}}{e^x}$.
- B) $f'(x) = \frac{e^{3x} + 6e^{2x} - 5e^x}{(e^x + 3)^2}$.
- C) $f'(x) = \frac{e^{3x} - 6e^{2x} - 5e^x}{(e^x + 3)^2}$.
- D) $f'(x) = \frac{e^{3x} + 6e^{2x} + 5e^x}{(e^x + 3)^2}$.

QUESTION 14 :

La fonction f est :

- A) strictement positive sur \mathbb{R} .
- B) strictement positive sur $[0, +\infty[$.
- C) strictement positive sur $[2, +\infty[$.
- D) strictement positive sur $[-2; 8]$.

QUESTION 15 :

La limite de la fonction f en $+\infty$ est égale à :

- A) 1.
- B) $\frac{-5}{3}$.
- C) $+\infty$.
- D) 0.

QUESTION 16 :

La limite de la fonction f en $-\infty$ est égale à :

- A) 1.
- B) $\frac{-5}{3}$.
- C) 0.
- D) $\frac{-3}{5}$.

QUESTION 17 :

La courbe représentative de la fonction f :

- A) admet la droite d'équation $y = 1$ comme asymptote.
- B) admet la droite d'équation $x = \frac{-5}{3}$ comme asymptote.
- C) admet la droite d'équation $y = \frac{-5}{3}$ comme asymptote.
- D) n'a pas d'asymptote.

QUESTION 18 : Une équation de la tangente à la courbe représentative de la fonction f au point d'abscisse 0 est :

- A) $y = \frac{3}{4}x - 1$.
- B) $y = \frac{3}{4}x$.
- C) $y = x - \frac{3}{4}$.
- D) $y = \frac{3}{4}x + 1$.

QUESTION 19 :

Une primitive F de f est définie sur \mathbb{R} par :

- A) $F(x) = (e^{2x} - 5) \ln(e^x + 3).$
- B) $F(x) = \frac{3e^x - 5x - 4 \ln(e^x + 3)}{3}.$
- C) $F(x) = (e^{2x} - 5) + \ln(e^x + 3).$
- D) $F(x) = \frac{\frac{e^{2x}}{2} - 5}{3x + e^x}.$

Partie IV

Soit l'équation différentielle du second ordre (E) : $9y'' + y = 0$, où y désigne une fonction de la variable x .

Soit f la solution de l'équation (E) telle que $f(0) = \frac{1}{2}$ et $f'(0) = \frac{-\sqrt{3}}{6}$.

QUESTION 20 :

Alors

- A) $f(x) = \frac{1}{2} \sin\left(\frac{x}{3}\right) + \frac{\sqrt{3}}{2} \cos\left(\frac{x}{3}\right).$
- B) $f(x) = \frac{1}{2} \cos\left(\frac{x}{3}\right) + \frac{\sqrt{3}}{2} \sin\left(\frac{x}{3}\right).$
- C) $f(x) = \frac{1}{2} \sin\left(\frac{x}{3}\right) - \frac{\sqrt{3}}{2} \cos\left(\frac{x}{3}\right).$
- D) $f(x) = \frac{1}{2} \cos\left(\frac{x}{3}\right) - \frac{\sqrt{3}}{2} \sin\left(\frac{x}{3}\right).$

QUESTION 21 :

C'est aussi

- A) $f(x) = \sin\left(\frac{x}{3} + \frac{5\pi}{6}\right).$
- B) $f(x) = \cos\left(\frac{x}{3} - \frac{5\pi}{6}\right).$
- C) $f(x) = \sin\left(\frac{x}{3} - \frac{5\pi}{6}\right).$
- D) $f(x) = \sin\left(\frac{-x}{3} + \frac{5\pi}{6}\right).$

QUESTION 22 :

Le nombre $f''(0)$ est égal à :

- A) $\frac{1}{4}.$
- B) $\frac{2}{9}.$
- C) $\frac{-1}{18}.$
- D) $\frac{1}{18}.$

QUESTION 23 :

La fonction f est :

- A) périodique de période $\frac{\pi}{3}.$
- B) périodique de période $3\pi.$
- C) paire.
- D) impaire.

QUESTION 24 :

Soit (u_n) une suite définie pour tout entier naturel non nul n , par

$$u_n = e^{\frac{1}{n}} \cos(n\pi).$$

Alors (u_n) :

- A) n'est pas strictement monotone.
- B) est strictement décroissante.
- C) est strictement croissante.
- D) admet 1 comme limite quand n tend vers $+\infty$.

QUESTION 25 :

Soit (u_n) une suite définie pour tout entier naturel n , par $u_n = e^n - n^3$.

Alors (u_n) :

- A) n'est pas strictement monotone.
- B) est strictement décroissante.
- C) est constante.
- D) admet $+\infty$ comme limite quand n tend vers $+\infty$.

N° CANDIDAT :

CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C - SESSION 2017-

Epreuve Ecrite obligatoire : MATHEMATIQUES
GRILLE DE REPONSE A REMETTRE A LA FIN DE L'EPREUVE

GRILLE DE REPONSES

ATTENTION : Le candidat apportera le plus grand soin au remplissage de la feuille de réponses en évitant correcteur et rature. Enfin il est rappelé que toute réponse inexacte entraînera une pénalité pour la question concernée.

Question 1	A	B	C	D	E
Question 2	A	B	C	D	E
Question 3	A	B	C	D	E
Question 4	A	B	C	D	E
Question 5	A	B	C	D	E
Question 6	A	B	C	D	E
Question 7	A	B	C	D	E
Question 8	A	B	C	D	E
Question 9	A	B	C	D	E
Question 10	A	B	C	D	E
Question 11	A	B	C	D	E
Question 12	A	B	C	D	E
Question 13	A	B	C	D	E
Question 14	A	B	C	D	E
Question 15	A	B	C	D	E

N° CANDIDAT :

CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C - SESSION 2017-

Epreuve Ecrite obligatoire : MATHEMATIQUES
GRILLE DE REPONSE A REMETTRE A LA FIN DE L'EPREUVE

GRILLE DE REPONSES

ATTENTION : Le candidat apportera le plus grand soin au remplissage de la feuille de réponses en évitant correcteur et rature. Enfin il est rappelé que toute réponse inexacte entraînera une pénalité pour la question concernée.

Question 16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E
Question 25	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A	B	C	D	E



**CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C – Session 2017 -**

**CONCOURS EXTERNE/INTERNE
Epreuve Optionnelle Obligatoire**

MATHEMATIQUES – PHYSIQUE

**Partie génie Mathématiques AC1_17_MP_1
Partie Physique AC1_17_PH_1**

Date de l'épreuve : 27 juin 2017
Durée de l'épreuve : 3 heures
**Coefficient : 6 (concours externe)
5 (concours interne)**

Ce sujet comporte :

- ⊖ Une page de garde Mathématiques
 - ⊖ 2 pages de consignes
 - ⊖ Sujet – Total 6 pages
 - ⊖ Une grille réponse Mathématiques à remettre à la fin de l'épreuve.

 - ⊖ Une page de garde Physique
 - ⊖ Une page de consignes
 - ⊖ Sujet – Total 5 pages
 - ⊖ Une grille réponse Physique à remettre à la fin de l'épreuve.
-



**CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C –Session 2017 -**

CONCOURS EXTERNE/INTERNE

Epreuve Optionnelle Obligatoire

MATHEMATIQUES

CALCULATRICE INTERDITE

Les réponses se feront sur le document de réponses

MATHEMATIQUES

Cette épreuve comporte 15 questions.

Tout dispositif électronique est INTERDIT (en particulier l'usage de la calculatrice).

Chaque question comporte au plus deux réponses exactes.

A chaque question numérotée de 1 à 15, correspond sur la feuille " Grille de réponses " une ligne de cases qui porte le même numéro.

Chaque ligne comporte 5 cases A, B, C, D, E.

Pour chaque ligne numérotée de 1 à 15, vous vous trouverez en face de 4 possibilités :

- 1) Soit vous décidez de ne pas traiter cette question : la ligne correspondante doit rester vierge.
- 2) Soit vous jugez que la question comporte une seule bonne réponse : vous devez faire une croix sur l'une des cases A, B, C, D.
- 3) Soit vous jugez que la question comporte deux réponses exactes : vous devez faire une croix sur deux des cases A, B, C, D et deux seulement.
- 4) Soit vous jugez qu'aucune des réponses proposées A, B, C, D n'est bonne : vous devez alors faire une croix sur E.

Chaque question rapporte 1 point.

Attention : Toute réponse fausse entraîne une pénalité dans la note ; une réponse fausse = -0,5.

Questions liées :

1 à 3

8 à 10

13 à 15

Les autres questions sont indépendantes.

L'espace est muni d'un repère orthonormal $(O; \vec{i}, \vec{j}, \vec{k})$. Soit (P) un plan d'équation cartésienne : $3x - y + z - 2 = 0$ et les points $A(0; 4; 1)$, $B(1; 5; -2)$.

QUESTION 1 :

Une représentation paramétrique de la droite (AB) est :

- A)
$$\begin{cases} x = 1 + t \\ y = 5 + t \\ z = -2 + 3t \end{cases} \quad (t \in \mathbb{R})$$
- B)
$$\begin{cases} x = 1 + t \\ y = 5 - t \\ z = -2 - 3t \end{cases} \quad (t \in \mathbb{R})$$
- C)
$$\begin{cases} x = 1 + 5t \\ y = 5 + 5t \\ z = -2 - 15t \end{cases} \quad (t \in \mathbb{R})$$
- D)
$$\begin{cases} x = 1 + t \\ y = 5 + t \\ z = -2 - 3t \end{cases} \quad (t \in \mathbb{R})$$

QUESTION 2 :

Alors :

- A) La droite (AB) et le plan (P) sont strictement parallèles.
- B) La droite (AB) et le plan (P) sont sécants.
- C) La droite (AB) est orthogonale au plan (P) .
- D) La droite (AB) est dans le plan (P) .

QUESTION 3 :

La droite (OB) coupe le plan (P) au point :

- A) $M(\frac{-1}{2}; \frac{-5}{2}; 1).$
- B) $M(-5; -1; 16).$
- C) $M(\frac{-1}{2}; \frac{5}{2}; -1).$
- D) $M(0; -1; 1).$

Si x est un nombre réel, on note indifféremment $\exp(x) = e^x$.

QUESTION 4 :

L'ensemble des solutions dans \mathbb{R} de l'équation $e^{2x} - (1 + e^3)e^x + e^3 = 0$ est :

- A) $S = \{-1; 3\}.$
- B) $S = \{0; 3\}.$
- C) $S = \{-1; -3\}.$
- D) $S = \{1; -3\}.$

QUESTION 5 :

L'ensemble des solutions dans \mathbb{R} de l'inéquation $\exp\left(\frac{5-x}{x+2}\right) \geq 1$ est :

- A) $S =]-2; 5].$
- B) $S =]2; 5].$
- C) $S = [-2; 5].$
- D) $S =]-2; 5[.$

QUESTION 6 :

La fonction f définie sur \mathbb{R} par $f(x) = (1 - x^2)e^{-x}$:

- A) est décroissante sur \mathbb{R} .
- B) est croissante sur \mathbb{R} .
- C) admet un minimum local sur \mathbb{R} .
- D) admet un maximum local sur \mathbb{R} .

QUESTION 7 :

Soit (U_n) une suite définie pour tout entier naturel non nul n , par $U_n = \frac{3^n}{n^3}$.

- A) La suite (U_n) est monotone.
- B) La suite (U_n) est majorée.
- C) La suite (U_n) est croissante.
- D) La suite (U_n) est convergente.

Deux amis Vetea et Marie se téléphonent très régulièrement. La durée d'une communication entre ces deux amis, exprimée en minutes, suit la loi uniforme sur l'intervalle $[0; 60]$.

Question 8 :

La probabilité qu'une communication n'excède pas 20 minutes est :

- A) $\frac{2}{3}$.
- B) $\frac{1}{3}$.
- C) $\frac{3}{4}$.
- D) $\frac{1}{2}$.

Question 9 :

Sachant qu'une communication dure depuis 10 minutes, la probabilité qu'elle n'excède pas 40 minutes est égale à :

- A) $\frac{3}{5}$.
- B) $\frac{1}{4}$.
- C) $\frac{2}{5}$.
- D) $\frac{2}{3}$.

QUESTION 10 :

La durée moyenne en minutes d'une communication entre ces deux amis est égale à :

- A) 20.
- B) 30.
- C) 40.
- D) 50.

QUESTION 11 :

On a :

- A) $\int_{-2}^2 \sqrt{4-x^2} dx = 4$.
- B) $\int_{-2}^2 \sqrt{4-x^2} dx = 4\pi$.
- C) $\int_{-2}^2 \sqrt{4-x^2} dx = \pi$.
- D) $\int_{-2}^2 \sqrt{4-x^2} dx = 2\pi$.

QUESTION 12 :

La moyenne de la fonction $x \mapsto \sin^2(x)$ sur l'intervalle $[0; 2\pi]$ est égale à :

- A) 1.
- B) 2.
- C) $\frac{1}{2}$.
- D) $\frac{2}{\pi}$.

Soit la fonction f définie sur \mathbb{R} par $f(x) = \ln(x + \sqrt{x^2 + 1})$ et (C) sa courbe représentative dans un repère orthonormal.

QUESTION 13 :

Alors :

- A) f est paire.
- B) f est impaire.
- C) f est ni paire ni impaire.
- D) (C) admet un axe de symétrie.

QUESTION 14 :

La limite de f en $-\infty$ est égale à :

- A) 0.
- B) $\ln 2$.
- C) \sqrt{e} .
- D) $+\infty$.

QUESTION 15 :

La fonction f est :

- A) strictement positive sur l'intervalle $\left[-\frac{1}{2}; \frac{3}{2}\right]$.
- B) strictement positive sur l'intervalle $\left[0; \frac{3}{2}\right]$.
- C) strictement positive sur l'intervalle $]0; +\infty[$.
- D) strictement positive sur \mathbb{R} .

N° CANDIDAT :

CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C - SESSION 2017-

Epreuve optionnelle obligatoire : MATHEMATIQUES (MP)
GRILLE DE REPONSE A REMETTRE A LA FIN DE L'EPREUVE

GRILLE DE REPONSES MATHEMATIQUES

ATTENTION : Le candidat apportera le plus grand soin au remplissage de la feuille de réponses en évitant correcteur et rature. Enfin il est rappelé que toute réponse inexacte entraînera une pénalité pour la question concernée.

Question 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 13	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 14	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E
Question 15	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	A	B	C	D	E



**CONCOURS DE L'AVIATION CIVILE
T.S.E.E.A.C –Session 2017 -**

CONCOURS EXTERNE/INTERNE

Epreuve Optionnelle Obligatoire

PHYSIQUE

CALCULATRICE INTERDITE

Les réponses se feront sur le document de réponses

Partie Physique

Cette épreuve comporte 15 questions

Aucun moyen de calcul n'est autorisé

CONSIGNES

Cette épreuve comporte 4 parties indépendantes :

Partie 1 : questions de 16 à 18

Partie 2 : questions de 19 à 21

Partie 3 : questions de 22 à 26

Partie 4 : questions de 27 à 30

Chaque question comporte au plus 2 réponses.

A chaque question numérotée de 16 à 30, correspond sur la feuille « GRILLE DES REPONSES » une ligne.

Chaque ligne comporte 5 cases A, B, C, D, E.

Pour chaque ligne vous avez 4 possibilités :

1. Vous décidez de ne pas traiter la question :
LA LIGNE DOIT RESTER VIERGE
2. Vous jugez qu'il y a une seule réponse exacte :
VOUS DEVEZ FAIRE UNE CROIX DANS L'UNE DES CASES A, B, C, D.
3. Vous jugez qu'il y a 2 réponses exactes :
VOUS DEVEZ FAIRE UNE CROIX DANS 2 DES CASES A, B, C, D
4. Vous jugez qu'aucune réponse proposée n'est exacte :
VOUS DEVEZ FAIRE UNE CROIX DANS LA CASE E
5. Si la question comporte 2 réponses exactes et que vous n'en cochez qu'une, votre réponse est considérée comme inexacte.

BAREME

Une bonne réponse rapporte 1 point.

Une réponse inexacte enlève 0,5 points.

L'absence de réponse est comptée 0 points

Si le total est négatif, la note est ramenée à zéro.

Le total est noté sur 15, puis ramené à une note sur 10

Constantes physique et aides au calcul:

Charge élémentaire : $q_e = 1,6 \times 10^{-19} \text{ C}$

Constante de Planck : $h = 6,6 \times 10^{-34} \text{ J} \cdot \text{s}$

Célérité de la lumière : $c = 3 \times 10^8 \text{ m} \cdot \text{s}^{-1}$

$\pi = 3.14$

Partie 1

L'effet Doppler

Dans les questions suivantes E est la source d'un signal sonore périodique et R est le récepteur du signal.

La fréquence et la période du signal émis et la vitesse de E sont indiquées par f_E , T_E , v_E .

La fréquence et la période du signal reçu et la vitesse de R sont indiquées par f_R , T_R , v_R .

Les mouvements de E ou R se font dans la direction (ER)

La célérité du signal est indiquée par v_s .

Toutes les vitesses sont mesurées dans un référentiel terrestre.

- Question 16 :

Sachant que la source s'éloigne du récepteur immobile :

- A. $T_R < T_E$
- B. $f_R < f_E$
- C. $v_E = v_s \frac{f_E - f_R}{f_R}$
- D. $\frac{f_R}{f_E} = (1 + \frac{v_E}{v_s})$

- Question 17 :

Sachant que le signal perçu en R, immobile, correspond au deuxième harmonique du signal émis par E

- A. E s'éloigne de R avec $v_E = 2v_s$
- B. E s'éloigne de R avec $v_E = \frac{1}{2} v_s$
- C. E s'approche de R avec $v_E = 2v_s$
- D. E s'approche de R avec $v_E = \frac{1}{2} v_s$

- Question 18 :

L'émetteur et le récepteur sont partiellement immergés.

La vitesse de propagation d'une onde sonore dans l'air est environ cinq fois moins importante que dans l'eau.

Soit f_R^{AIR} la fréquence du signal se propageant dans l'air et reçue par R.

Soit f_R^{EAU} la fréquence du signal se propageant dans l'eau et reçue par R.

Sachant que la source se rapproche du récepteur :

- A. $f_R^{EAU} = f_R^{AIR}$
- B. $f_R^{EAU} < f_R^{AIR}$
- C. $f_R^{EAU} > f_R^{AIR}$
- D. $f_R^{EAU} \approx 5 f_R^{AIR}$

Partie 2

L'effet Doppler-Fizeau

- Question 19 :

- A. Le « redshift » (décalage vers le rouge) peut être observé dans le spectre d'une étoile ou d'une galaxie qui se rapproche de la terre
- B. Le « bluishift » (décalage vers le bleu) peut être observé dans le spectre d'une étoile ou d'une galaxie qui s'éloigne de la terre
- C. L'effet Doppler-Fizeau permet de connaître le vecteur vitesse d'une étoile si dans son spectre on repère des raies caractéristiques de certains atomes.
- D. La formule de l'effet Doppler pour les ondes électromagnétiques est la même que pour les ondes sonores si on néglige les effets relativistes.

Si un observateur se rapproche d'une source d'onde électromagnétique à une vitesse v non négligeable par rapport à celle de propagation de l'onde (c) on doit tenir compte des effets de la relativité restreinte.

En particulier la dilatation du temps impose que la période de l'onde électromagnétique perçue par l'observateur est celle calculée par l'effet Doppler multipliée par le facteur γ .

La période et la fréquence de l'onde perçue par l'observateur sont notées $T_{perçue}$, $f_{perçue}$

La période et la fréquence de l'onde émise par la source sont notées $T_{émise}$, $f_{émise}$

- Question 20 :

- A. $f_{perçue} = f_{émise} \gamma (1 - \frac{v}{c})$
- B. $T_{perçue} = T_{émise} \gamma (1 - \frac{v}{c})$
- C. $f_{perçue} = f_{émise} \gamma (1 - \frac{c}{v})$
- D. $T_{perçue} = T_{émise} \gamma (1 - \frac{c}{v})$

• Question 21 :

Le coefficient γ pouvant s'écrire : $\gamma = \frac{1}{\sqrt{1-\frac{v^2}{c^2}}} = \frac{1}{\sqrt{1+\frac{v}{c}}} \times \frac{1}{\sqrt{1-\frac{v}{c}}}$

- A. $f_{perçue} = f_{émise} \frac{\sqrt{v+c}}{\sqrt{v-c}}$
- B. $f_{perçue} = f_{émise} \frac{\sqrt{c-v}}{\sqrt{c+v}}$
- C. $f_{émise} = f_{perçue} \frac{\sqrt{c+v}}{\sqrt{c-v}}$
- D. $f_{perçue} = f_{émise} \frac{\sqrt{c+v}}{\sqrt{c-v}}$

Partie 3

Il est possible de refroidir des atomes avec des lasers. En effet lorsqu'un photon est absorbé par un atome en mouvement, en appliquant la conservation de la quantité de mouvement, la vitesse de l'atome peut diminuer.

• Question 22 :

- A. La quantité de mouvement du photon est dirigée dans le sens de propagation du photon
- B. La quantité de mouvement du photon et de l'atome se calculent avec la formule

$$\vec{p} = \frac{hc}{\nu}$$

- C. Si la vitesse du photon et de l'atome ont la même direction et sens opposés le ralentissement est maximal
- D. La quantité de mouvement du photon se calcule avec la formule

$$p = \frac{\lambda}{h}$$

L'atome de rubidium au repos absorbe des photons d'une longueur d'onde $\lambda_0 = 780 \text{ nm}$

• Question 23 :

L'ordre de grandeur de la transition énergétique associée à cette absorption est de

- A. 1eV
- B. 1keV
- C. 1J
- D. 10^{-10} J

• Question 24 :

La quantité de mouvement d'un photon de longueur d'onde $\lambda_0 = 780 \text{ nm}$ est comprise entre :

- A. $7 \times 10^{-28} \text{ J} \cdot \text{m} \cdot \text{s}^{-1}$ et $9 \times 10^{-28} \text{ J} \cdot \text{m} \cdot \text{s}^{-1}$
- B. $5 \times 10^{-28} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$ et $1 \times 10^{-27} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$
- C. $7 \times 10^{-37} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$ et $9 \times 10^{-37} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$
- D. $1 \times 10^{27} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$ et $2 \times 10^{27} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$

Dans l'expérience du ralentissement par laser, les atomes de rubidium ($m = 1.44 \times 10^{-25} \text{ kg}$) sont à l'état gazeux et leur vitesse moyenne est d'environ $150 \text{ m} \cdot \text{s}^{-1}$.

• Question 25 :

La quantité de mouvement moyenne de l'atome de rubidium est :

- A. Entre 20000 et 30000 fois plus grande que celle du photon absorbé
- B. $2.16 \times 10^{-23} \text{ J} \cdot \text{m} \cdot \text{s}^{-1}$
- C. plus petite que celle du photon absorbé
- D. $2.16 \times 10^{-23} \text{ kg} \cdot \text{m} \cdot \text{s}^{-1}$

L'atome étant en mouvement, il faut tenir compte de l'effet Doppler. Le photon émis par le laser sera absorbé si sa fréquence *perçue* par l'atome correspond à λ_0

• Question 26 :

Pour que l'atome soit ralenti par l'absorption du photon émis par le laser

- A. La longueur d'onde du laser doit être plus grande que λ_0
- B. La longueur d'onde du laser doit être plus petite que λ_0
- C. La longueur d'onde du laser doit être exactement égale à λ_0
- D. L'énergie du photon doit être plus petite que celle de la transition énergétique de l'atome

Partie 4

Soit un réservoir rempli d'eau douce de forme cylindrique de hauteur $h = 10 \text{ m}$ et diamètre $d = 12 \text{ m}$. Sa base est posée sur une plateforme à une hauteur $H = 45 \text{ m}$ du sol.

• Question 27 :

- A. Le réservoir contient environ 113 tonnes d'eau
- B. Le centre de gravité de la masse d'eau est à 45 m du sol

- C. L'énergie potentielle de pesanteur de la masse d'eau par rapport au sol est de 565.2 MW
- D. L'énergie nécessaire pour remplir le réservoir avec de l'eau pompée au niveau du sol est plus grande que 565.2 MJ

Un tuyau vertical relie la base du réservoir au sol et une vanne commandée par un dispositif électronique permet d'avoir un débit d'eau constant de 600 l.min^{-1} au niveau du sol.

L'eau sortant au niveau du sol permet de faire tourner une turbine.

• Question 28 :

- A. Il faut 1 jour 8 heures et 24 min pour vider le réservoir
- B. Le réservoir se vidant, la vanne se ferme de plus en plus
- C. Le réservoir se vidant, la vanne s'ouvre de plus en plus
- D. La puissance disponible au niveau de la turbine est de l'ordre de 5kW

L'énergie par unité de masse du pétrole est de 12 kWh.kg^{-1} .

• Question 29 :

- A. Le kWh est une unité de puissance
- B. L'énergie par unité de masse du pétrole est de 4.32 MJ.kg^{-1}
- C. Environ 13 kg de pétrole peuvent fournir la même quantité d'énergie que l'eau stockée dans le réservoir
- D. Il faut utiliser entre 300g et 500g de pétrole par heure pour avoir la même puissance que celle disponible à la turbine.

Voici les caractéristiques d'un parc de batteries :

- Tension nominale 24V
- Capacité totale 3200Ah

Rappels

- 1Ah est la quantité de charge électrique fournie par la batterie lorsqu'elle débite un courant de 1A pendant 1h.
- Un courant de 1A sous une tension de 1V fournit une puissance de 1W

• Question 30 :

Les batteries sont considérées idéales (rendements= 100%)

- A. Un ampère-heure est égal à 60 coulombs
- B. La puissance stockée dans le parc est de 76.8 kWh
- C. L'énergie disponible dans le parc est de 276.48 MJ
- D. Le parc fournit une énergie égale à celle de l'eau stockée dans le réservoir.

N° CANDIDAT :

GRILLE DE REPONSES PARTIE PHYSIQUE (à rendre)

QUESTION 16	A	B	C	D	E
QUESTION 17	A	B	C	D	E
QUESTION 18	A	B	C	D	E
QUESTION 19	A	B	C	D	E
QUESTION 20	A	B	C	D	E
QUESTION 21	A	B	C	D	E
QUESTION 22	A	B	C	D	E
QUESTION 23	A	B	C	D	E
QUESTION 24	A	B	C	D	E
QUESTION 25	A	B	C	D	E
QUESTION 26	A	B	C	D	E
QUESTION 27	A	B	C	D	E
QUESTION 28	A	B	C	D	E
QUESTION 29	A	B	C	D	E
QUESTION 30	A	B	C	D	E