

BREVET DE TECHNICIEN SUPÉRIEUR

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

Option A – Informatique et Réseaux Épreuve

E4

ÉTUDE ET CONCEPTION DE RÉSEAUX INFORMATIQUES

SESSION 2025

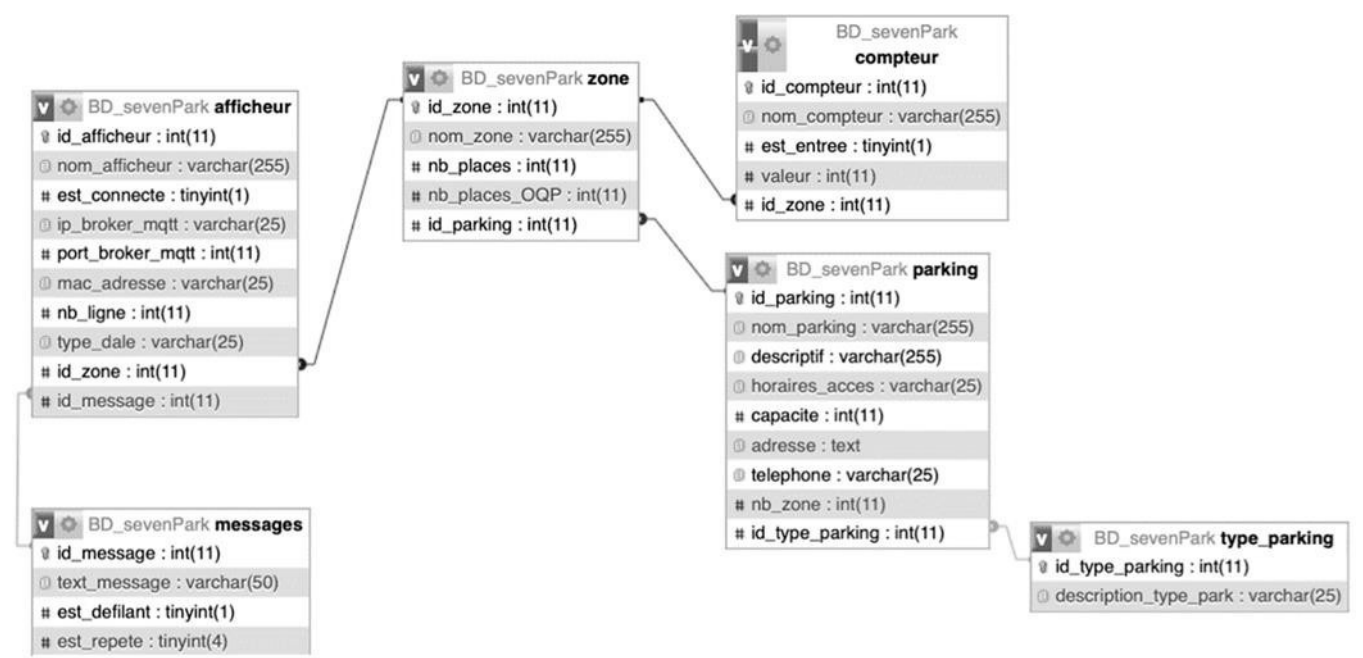
**Durée : 6 heures Coefficient
: 4**

DOCUMENTS TECHNIQUES

DT1 - Base de données du système d'étude	2 à 3
DT2 - Notice d'Installation Système de comptage (ESP 32)	4
DT3 - Afficheur : liste des commandes.....	5 à 6
DT4 - Table ASCII de 0 à 127	7
DT5 - Hameçonnage ou usurpation d'identité.....	8
DT6 - Mots de passe	9
DT7 - Sécuriser les postes de travail.....	10
DT8 - Guide de l'ANSSI sur la sauvegarde des systèmes.....	11
DT9 - Bloc à placer dans document réponse DR6.....	12
DT10 - Sécurisation d'un commutateur.....	13
DT11 - Principaux types de données MySQL/MariaDB	14
DT12 - Rappel de la syntaxe SQL.....	15
DT13 - Logiciel d'affichage.....	16 à 17
DT14 - Notice d'Installation Système de comptage avec Boucle au Sol (ESP 32)	18
DT15 - Détecteur de boucle : ProLoop2.....	19 à 20
DT16 - Protéger le réseau informatique	21
DT17 - Rappels et commandes de base sur les commutateurs Cisco	22 à 23
DT18 - Le RGPD, qu'est-ce que c'est ?	24 à 25
DT19 - Documentation commande mysqldump.....	26
DT20 - Documentation sur fichier « crontab »	27
DT21 - Réponse d'un « chatbot » à une question sur la réplication du SGBDR MariaDB	28

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE		Session 2025
OPTION INFORMATIQUE ET RÉSEAUX		
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC1 sur 28

DT1 - Base de données du système d'étude



Extrait modèle relationnel de la BDD

Remarque :

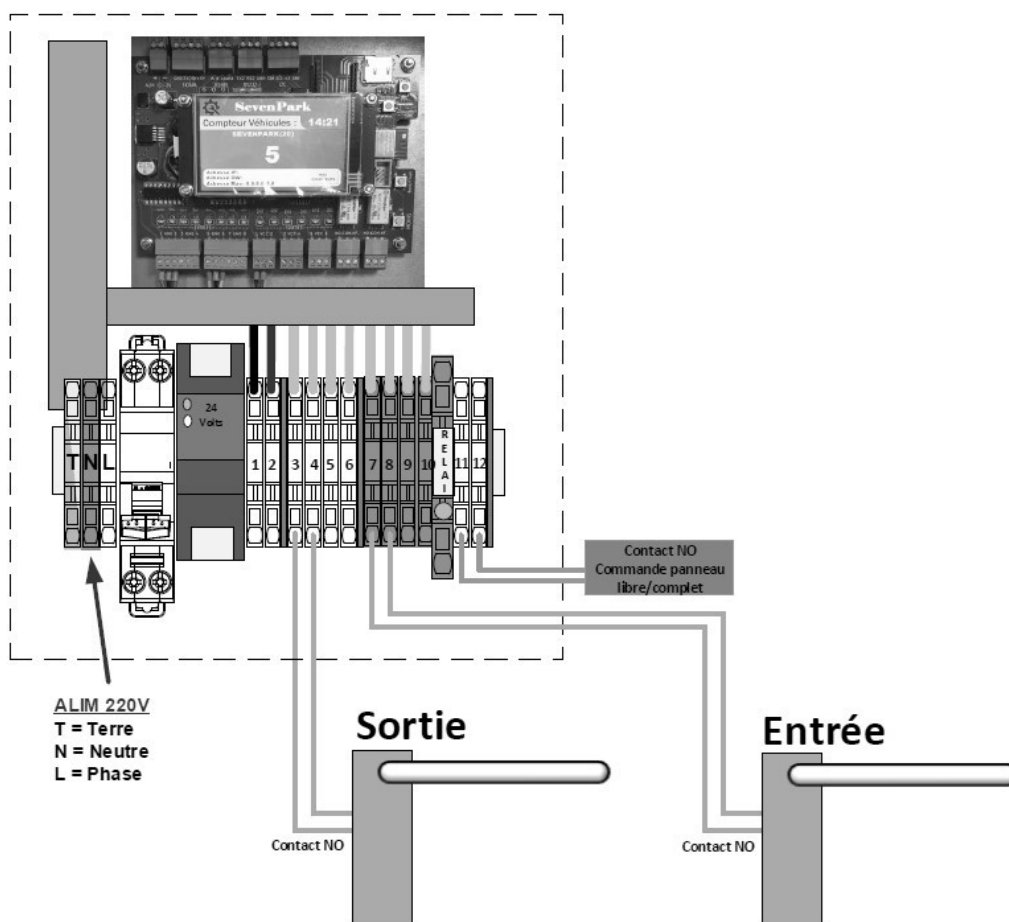
nb_places_OQP est le nombre de places occupées (nombre de véhicules actuellement dans la zone)

Extrait du dictionnaire de données :

Nom du champ	Table	Type	Champ obligatoire ?	Valeur par défaut	Rôle
horaires_acces	parking	VARCHAR(25)	non		Heures d'ouverture du parking
capacite	parking	INT	oui		Nombre de places maximum du parking
nb_zone	parking	INT	oui		Nombre de zones du parking
nb_places_OQP	zone	INT	non	0	Nombre de véhicules actuellement dans la zone
Nb_places	zone	INT	oui		Nombre de places total de la zone
est_connecte	afficheur	TINYINT (booleen)	non	0	Indique si l'afficheur est connecté, si oui les champs "ip_broker_MQTT", "port_broker_MQTT" et "mac_adresse" seront renseignés
ip_broker_mqtt	afficheur	VARCHAR(25)	non		Adresse IP du broker pour le protocole MQTT
port_broker_mqtt	afficheur	INT	non		Port du broker pour le protocole MQTT
mac_adresse	afficheur	VARCHAR(25)	non		Adresse MAC associée à l'afficheur
est_defilant	afficheur	TINYINT (booleen)	non	0	Indique si le message est défilant si = 1
est_repete	afficheur	TINYINT (booleen)	non	1	Indique si le message est répété si = 1
est_entre	compteur	TINYINT (booleen)	non	0	Lorsque vaut "1" = alors compteur entrée, sinon compteur de sortie

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC3 sur 28

NOTICE D'INSTALLATION SYSTEME DE COMPTAGE



- 1 & 2 - Alimentation 24 v
- 3 à 6 - Entrée Comptage (contact Normalement Ouvert)
Un véhicule sortant, ajoute une place libre dans le parking
- 7 à 10 - Entrée Décomptage (contact Normalement Ouvert)
Un véhicule entrant, enlève une place libre dans le parking
- 11 & 12 - Contact No de commande panneau LED

S.A.R.L SEVEN PARK, 110 Route de la Baronne
Le sophora -lot 16, Code Naf : 4329B
Du Lundi au Vendredi de 8h30 à 18h
Contact@sevenpark.fr
www.sevenpark.fr



CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC4 sur 28

DT3 - Afficheur : liste des commandes

Commande n°	Description	Détails spécifiques
0	Redémarrage de l'afficheur	
1	CPT VISITEUR 2 LIGNES	Affiche Logo 'P' suivi du nombre de places.
2	CPT ABONNE 2 LIGNES	Met à jour le compteur correspondant aux places réservées aux utilisateurs abonnés.
3	CPT PMR 2 LIGNES	Met à jour le compteur correspondant aux places réservées aux utilisateurs à mobilité réduite (PMR).
9	ACCUEIL DEFILEMENT	Affiche le nom du parking en continu avec défilement.
10	ACCUEIL	Affiche le nom du parking sur 2 lignes sans défilement.
11	LIBRE 2 LIGNES	Affiche le logo 'P' sur la gauche, suivi de 'PARKING LIBRE' en vert sur 2 lignes.
12	COMPLET 2 LIGNES	Affiche le logo 'P' sur la gauche, suivi de 'PARKING COMPLET' en rouge sur 2 lignes.
13	OUVERT 2 LIGNES	Affiche le logo 'P' sur la gauche, suivi de 'PARKING OUVERT' en vert sur 2 lignes.
14	FERME 2 LIGNES	Affiche le logo 'sens interdit', suivi de 'PARKING FERME' en rouge sur 2 lignes.
15	LIBRE DEFILEMENT	Affiche logo 'P', suivi 'LIBRE' en vert, en continu, avec défilement.
16	COMPLET DEFILEMENT	Affiche 'COMPLET' en rouge, en continu, avec défilement.
17	OUVERT DEFILEMENT	Affiche 'OUVERT' en vert, en continu, avec défilement.
18	FERME DEFILEMENT	Affiche 'FERME' en rouge, en continu, avec défilement.
20	PLACE VISITEUR 2 LIGNES	Affiche 'PLACES LIBRES' en vert, sur 2 lignes à gauche, suivi de la donnée contenue dans la trame (blanc).
21	PLACE ABONNES 2 LIGNES	Affiche 'PLACES ABONNES' en vert clair, sur 2 lignes à gauche suivi de la donnée contenue dans la trame (blanc).
22	PLACE PMR 2 LIGNES	Affiche 'PLACES PMR' en bleu sur 2 lignes à gauche suivi de la donnée contenue dans la trame (blanc).
23	PLACE VISITEURS DEFILEMENT	Affiche 'PLACES LIBRES' (en blanc) suivi de la donnée contenue dans la trame. Si la donnée est inférieure à 10, elle sera affichée en rouge, sinon en vert. Le tout défile en continu.
24	PLACE ABONNES DEFILEMENT	Affiche 'PLACES ABONNES' (vert clair) suivi de la donnée contenue dans la trame. Si la donnée est inférieure à 10, elle sera affichée en rouge, sinon en vert. Le tout défile en continu.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC5 sur 28

25	PLACE PMR DEFILEMENT	Affiche 'PLACES PMR' (bleu) suivi de la donnée contenue dans la trame. Si la donnée est inférieure à 10, elle sera affichée en rouge, sinon en vert. Le tout défile en continu.
36	MESSAGE LIVE	Affiche uniquement la ligne 1 en blanc, avec défilement continu. Aucune donnée n'est requise.
37	MESSAGE LIVE 2 LIGNES	Affiche ligne 1 et ligne 2 l'une en dessous de l'autre. Aucune donnée n'est requise. Cet affichage peut être paramétré par les commandes n°42,43,45 et 46.
38	CPT LIVE 1 LIGNE	Affiche la ligne 1, avec défilement continu.
40	TEXT MESS LIGNE 1	Définit le texte de la ligne 1.
41	TEXT MESS LIGNE 2	Définit le texte de la ligne 2.
42	COULEUR LIGNE 1	Définit la couleur de la ligne 1 : 0 - vert ; 1 - bleu ; 2 - rouge ; 3 - blanc ; 4 - vert clair ; 5 - noir.
43	COULEUR LIGNE 2	Définit la couleur de la ligne 2 : 0 - vert ; 1 - bleu ; 2 - rouge ; 3 - blanc ; 4 - vert clair ; 5 - noir.
45	COORDONNEE X de la ligne 1 (en pixels)	Permet de déterminer la position de l'affichage de la ligne 1 à partir de la gauche. (0 : alignement à gauche ; 1 : décalage de 1 pixel ; ...).
46	COORDONNEE X de la ligne 2 (en pixels)	Permet de déterminer la position de l'affichage de la ligne 2 à partir de la gauche. (0 : alignement à gauche ; 1 : décalage de 1 pixel ; ...).

Message 'LIVE' : le message 'LIVE' est un message non prédéfini dans l'afficheur. Il est constitué de 2 lignes appelées 'ligne 1' et 'ligne2'. Chaque ligne peut avoir sa propre couleur, et être positionnée précisément.

Exemple : sur le bus RS485, on envoie la trame : **3/25/15**.

Explications :

- Numéro de l'afficheur : 3
- Numéro de la commande exécutée : 25
- Donnée : 15

Cette trame permet donc d'exécuter la commande N°25 sur l'afficheur N°3. Le message affiché sera 'PLACES PMR' en bleu, suivi du nombre « 15 » écrit en vert. L'ensemble de ce message défile en continu.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC6 sur 28

DT4 - Table ASCII de 0 à 127

Dec	Name	Char	Dec	Char	Dec	Char	Dec	Char
0	Null	Nul	32	Space	64	@	96	`
1	Start of heading	SCH	33	!	65	A	97	a
2	Start of text	STX	34	"	66	B	98	b
3	End of text	ETX	35	#	67	C	99	c
4	End of xmit	EOT	36	\$	68	D	100	d
5	Enquiry	ENQ	37	%	69	E	101	e
6	Acknowledge	ACK	38	&	70	F	102	f
7	Bell	BEL	39	'	71	G	103	g
8	backspace	BS	40	(	72	H	104	h
9	Horizontal tab	HT	41	)	73	I	105	i
10	Line feed	LF	42	*	74	J	106	j
11	Vertical tab	VT	43	+	75	K	107	k
12	Form feed	FF	44	,	76	L	108	l
13	Carriage feed	CR	45	-	77	M	109	m
14	Shift out	SO	46	.	78	N	110	n
15	Shift in	SI	47	/	79	O	111	o
16	Data line esc.	DLE	48	0	80	P	112	p
17	Device control 1	DC1	49	1	81	Q	113	q
18	Device control 2	DC2	50	2	82	R	114	r
19	Device control 3	DC3	51	3	83	S	115	s
20	Device control 4	DC4	52	4	84	T	116	t
21	Neg ack.	NAK	53	5	85	U	117	u
22	Sync. idle	SYN	54	6	86	V	118	v
23	End of xmit blk	ETB	55	7	87	W	119	w
24	Cancel	CAN	56	8	88	X	120	x
25	End of medium	EM	57	9	89	Y	121	y
26	Substitute	SUB	58	:	90	Z	122	z
27	Escape	ESC	59	;	91	[	123	{
28	File separator	FS	60	<	92	\	124	
29	Group separator	GS	61	=	93	]	125	}
30	Record sep.	RS	62	>	94	^	126	~
31	Unit separator	US	63	?	95	_	127	DEL

DT5 - Hameçonnage ou usurpation d'identité

Comment repérer un hameçonnage ou une usurpation d'identité par messagerie ou email ?

- **est-ce que le message/courriel vous est réellement destiné ?**
 - Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés ;
 - Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.
- **attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact ;
- **soyez attentif au niveau de langage du courriel** : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration...) ;
- **vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime ;
- **méfiez-vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code de carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel, même sur demande d'une personne qui annonce faire partie de votre entourage ;
- **l'adresse de messagerie source n'est pas un critère fiable** : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami (par exemple pour récupérer l'accès à son compte), contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Comment réagir ?

- n'ouvrez surtout pas les pièces jointes et ne répondez pas ;
- supprimez le message puis videz la corbeille ;
- s'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Comment s'en prémunir ?

- utilisez un logiciel de filtre antipourriel ou activez l'option d'avertissement contre les sites dangereux présents sur la plupart des navigateurs ;
- installez un antivirus et mettez-le à jour ;
- désactivez le volet de prévisualisation des messages ;
- lisez vos messages en mode de texte brut.

(Source : site web CNIL)

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC8 sur 28

DT6 - Mots de passe

Mots de passe, pour maîtriser sa sécurité et se protéger des attaques (force brute ou autre).

L'authentification des utilisateurs accédant à un système informatique est un des fondamentaux de la sécurité informatique.

Ce guide de portée très large, élaboré par l'ANSSI avec la contribution de la CNIL, constitue une référence pour l'élaboration de mesures d'authentification, essentielles pour garantir la sécurité des traitements de données personnelles, en application des articles 5 et 32 du RGPD.

Les principales recommandations qui sont mises en avant dans ce guide sont résumées ci-après :

- mener une analyse de risque lors de la mise en place de moyens d'authentification ;
- privilégier l'utilisation de l'authentification multi facteur ;
- privilégier l'utilisation de l'authentification reposant sur un facteur de possession ;
- adapter la robustesse d'un mot de passe à son contexte d'utilisation ;
- utiliser un coffre-fort de mots de passe ;

(Source : site web de la CNIL)

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC9 sur 28

DT7 - Sécuriser les postes de travail

Prévenir les accès frauduleux, l'exécution de programmes malveillants (ex. : virus) ou la prise de contrôle à distance, notamment via Internet.

Les précautions élémentaires

- prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné ;
- installer un « **pare-feu** » (« *firewall* ») logiciel sur le poste et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail ;
- utiliser des **antivirus régulièrement mis à jour** ;
- **déployer les mises à jour de sécurité au plus tôt**, le cas échéant après les avoir testées. Les mises à jour venant corriger des failles critiques publiques doivent d'autant plus être installées sans délai ;
- limiter les droits des utilisateurs au strict minimum en fonction de leurs besoins sur les postes de travail ;
- **favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé, accessible via le réseau interne de l'organisme** plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation ;
- **effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation** à une autre personne ;
- pour les **supports amovibles** (ex. : clés USB, disques durs externes) :
 - sensibiliser les utilisateurs aux risques liés à l'utilisation de support amovible, en particulier s'ils proviennent de l'extérieur ;
 - **limiter la connexion de supports mobiles** à l'indispensable ;
 - désactiver l'exécution automatique (« *autorun* ») depuis les supports amovibles.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC10 sur 28

DT8 - Guide de l'ANSSI sur la sauvegarde des systèmes

Lutte contre les rançongiciels (ANSSI-BP-100 du 18/10/2023)

1. Contexte

La menace liée aux rançongiciels est prégnante à la date de publication de ce document.

Toute entité peut subir une attaque opportuniste ou ciblée d'un groupe cybercriminel. La sauvegarde des systèmes d'information, initialement utile dans le cas d'incidents opérationnels, est aujourd'hui indispensable pour répondre efficacement aux incidents de sécurité.

Il est fréquent qu'un attaquant tente de chiffrer, d'effacer ou de rendre indisponible l'infrastructure de sauvegarde, dans le but de ralentir la reconstruction du SI impacté et donc d'augmenter ses chances d'obtenir la rançon.

2. Recommandations

2.1 Architecture :

- les serveurs de sauvegarde doivent être cloisonnés et positionnés au sein du SI d'administration, ou au moins dans une zone réseau distincte de la zone de production hébergeant les serveurs sauvegardés ;
- les flux de sauvegarde doivent transiter au sein du réseau d'administration ;
- les flux de sauvegarde doivent transiter au sein d'un sous-réseau logique dédié (VLAN) ;
- il est recommandé de dédier une instance de serveur de sauvegarde et un magasin de données par niveau de sensibilité des données et/ou applications ;
- les serveurs hébergeant l'infrastructure de sauvegarde ne doivent pas faire partie d'un domaine Windows (Active Directory) de production. Ils doivent disposer d'un système d'authentification indépendant (comptes locaux, annuaire dédié à l'administration) ;
- les flux de sauvegarde doivent être filtrés strictement au moyen d'un pare-feu interne.

2.2 Opérations

- il est indispensable de mettre en place une sauvegarde hors ligne (ou au moins hors site en ligne sous certaines conditions) même si celle-ci est moins fréquente que les sauvegardes locales régulières en ligne ;
- chaque instance de sauvegarde doit disposer de comptes d'administrateurs dédiés ;
- les comptes d'administrateurs pour la sauvegarde doivent être nominatifs et dédiés ;
- l'ensemble des composants de l'infrastructure de sauvegarde doit être mis à jour de manière proactive (logiciel de sauvegarde, micrologiciels, etc.). Il est recommandé de suivre les CVE (Common Vulnerabilities and Exposures) et les bulletins d'alertes fournis par l'éditeur de la solution.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC11 sur 28

DT9 - Bloc à placer dans document réponse DR6

Principe de l'attaque		Objectif de l'attaque		Recommandations aux employés		Moyen de protection que l'entreprise doit mettre en place	
Envoyer un mail en se faisant passer pour un organisme connu (banque, assurance ...), en demandant au destinataire de fournir des données sensibles.	Bloc 1	Récupérer des données sensibles pour s'introduire dans le compte de la personne ciblée et pouvoir réaliser des virements bancaires en son nom ou celui de son entreprise.	Bloc 6	- Utiliser des mots de passe complexes - Ne pas utiliser le même mot de passe partout. - Utiliser un gestionnaire de mots de passes	Bloc 11	Installer un antivirus et un pare-feu et les mettre à jour régulièrement.	Bloc 16
Tenter toutes les combinaisons possibles ou utiliser un dictionnaire de mot de passe.	Bloc 2	Deviner le mot de passe. Pour déverrouiller un accès protégé par mot de passe.	Bloc 7	- Ne pas suivre les liens et ne pas ouvrir les pièces jointes des mails suspects - Ne jamais fournir de coordonnées bancaires ou mot de passe par mail - Prévenir le service informatique	Bloc 12	Activer le filtre antispam.	Bloc 17
Réception d'un message avec pièce jointe activant un virus qui va bloquer l'équipement informatique en chiffrant son contenu.	Bloc 3	Faire de la publicité à moindre prix.	Bloc 8	- Ne jamais ouvrir un mail douteux ou dont on ne connaît pas la provenance. - Ne pas payer - Prévenir le responsable informatique - Déposer une plainte	Bloc 13	Politique de mot de passe (longueur, complexité, durée, etc.)	Bloc 19
Réception de <u>courrier électronique</u> à des destinataires ne l'ayant pas sollicité.	Bloc 4	Faire payer une rançon pour débloquent (ou pas) le contenu crypté	Bloc 9	- Ne pas ouvrir le mail - Ne pas acheter les produits proposés par le spam.	Bloc 14	Politique de sauvegarde hors ligne régulière des données	Bloc 20
Réception d'un message avec pièce jointe activant un virus.	Bloc 5	Détruire des données, bloquer l'ordinateur	Bloc 10	- Ne jamais ouvrir un mail douteux ou dont on ne connaît pas la provenance.	Bloc 15		

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC12 sur 28

DT10 - Sécurisation d'un commutateur

Recommandations pour la sécurisation d'un commutateur (No DAT-NT-25/ANSSI/SDE/NP - 24 juin 2016)

Extrait des recommandations Importantes

R2 - Mettre en place une séparation physique entre les réseaux d'administration et les réseaux de métier.

R2 - Au minimum, prévoir un cloisonnement logique utilisant des VLAN pour appliquer cette séparation.

R10 - Prendre les mesures nécessaires au sein du SI afin de n'autoriser l'accès à l'interface d'administration des commutateurs qu'aux administrateurs, notamment par l'utilisation de filtrage au niveau des pare-feu.

R10 - Si cela n'est pas possible, la mise en place des ACL sur le commutateur peut être envisagée en tant que mesure palliative.

R24 - Lorsqu'il n'est pas possible de mettre en place une séparation physique, il est recommandé de cloisonner son système d'information de façon cohérente grâce à l'utilisation des VLAN tout en respectant une logique utilité/simplicité dans le choix de la segmentation.

R28 - Le VLAN par défaut ne doit jamais être utilisé.

R31 - Le routage inter VLAN doit être assuré par des équipements de niveau 3. Celui-ci doit donc être désactivé sur les commutateurs d'accès.

R34 - Désactiver les ports inutilisés sur les commutateurs.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC13 sur 28

DT11 - Principaux types de données MySQL/MariaDB

Data Type	Storage Size (bytes)	Description
String Data Types		
CHAR(s)	s	A FIXED length string (can contain letters, numbers, and special characters). The s parameter specifies the column length in characters - can be from 0 to 255. Default is 1
VARCHAR(s)	s+1	A VARIABLE length string (can contain letters, numbers, and special characters). The s parameter specifies the maximum column length in characters - can be from 0 to 65535
TEXT	String length +2	Holds a string with a maximum length of 65,535 bytes
Numeric Data Types		
TINYINT	1	A very small integer. Signed range is from -128 to 127. Unsigned range is from 0 to 255.
SMALLINT	2	A small integer. Signed range is from -32768 to 32767. Unsigned range is from 0 to 65535.
INT	4	A medium integer. Signed range is from -2147483648 to 2147483647. Unsigned range is from 0 to 4294967295.
BIGINT	8	A large integer. Signed range is from -9223372036854775808 to 9223372036854775807. Unsigned range is from 0 to 18446744073709551615.
FLOAT	4	A floating point number
DOUBLE	8	A normal-size floating point number
Date and Time Data Types		
DATETIME	8	A date and time combination. Format: YYYY-MM-DD hh:mm:ss. The supported range is from '1000-01-01 00:00:00' to '9999-12-31 23:59:59'
TIMESTAMP	4	A timestamp. TIMESTAMP values are stored as the number of seconds since the Unix epoch ('1970-01-01 00:00:00' UTC). Format: YYYY-MM-DD hh:mm:ss. The supported range is from '1970-01-01 00:00:01' UTC to '2038-01-09 03:14:07' UTC

DT12 - Rappel de la syntaxe SQL

Sélectionner toutes les informations d'une table	SELECT * FROM nomTable ;
Sélectionner des champs d'une table	SELECT nomChamp1, nomChamp2 FROM nomTable1 ;
Sélectionner des champs d'une table et ajouter un champ calculé	SELECT nomChamp1, nomChamp2, (nomChamp3*nomChamp4) AS Total FROM nomTable1 ;
Sélectionner des enregistrements d'une table correspondant à deux critères	SELECT nomChamp1, nomChamp2 FROM nomTable1 WHERE nomChamp1='Nice' AND nomChamp2=45 ;
Sélectionner sur plusieurs tables (jointure)	<u>Jointure Classique :</u> SELECT nomTable1.nomChamp1, nomChamp2 FROM nomTable1, nomTable2 WHERE nomTable1.nomChamp1=nomTable2.nomChamp1 AND nomChamp3 = 'Paris'; <u>Jointure normalisée :</u> SELECT nomTable1.nomChamp1, nomChamp2 FROM nomTable1 JOIN nomTable2 ON nomTable1.nomChamp1=nomTable2.nomChamp1 WHERE nomChamp3 = 'Paris';
Ajouter des données dans une table	INSERT INTO nomTable (nomChamp1, nomChamp2) VALUES('Marseille', 48) ;
Mettre à jour les données d'une table	UPDATE nomTable SET nomChamp2=21+nomChamp2 WHERE nomChamp1='Marseille';
Ajouter des champs à la définition d'une table	ALTER TABLE nomTable ADD nomChamp1 TypeChamp1, ADD nomChamp2 TypeChamp2 ;
Compter le nombre d'enregistrements de la table	SELECT COUNT(nomChamp1) From nomTable ;

DT13 - Logiciel d’affichage

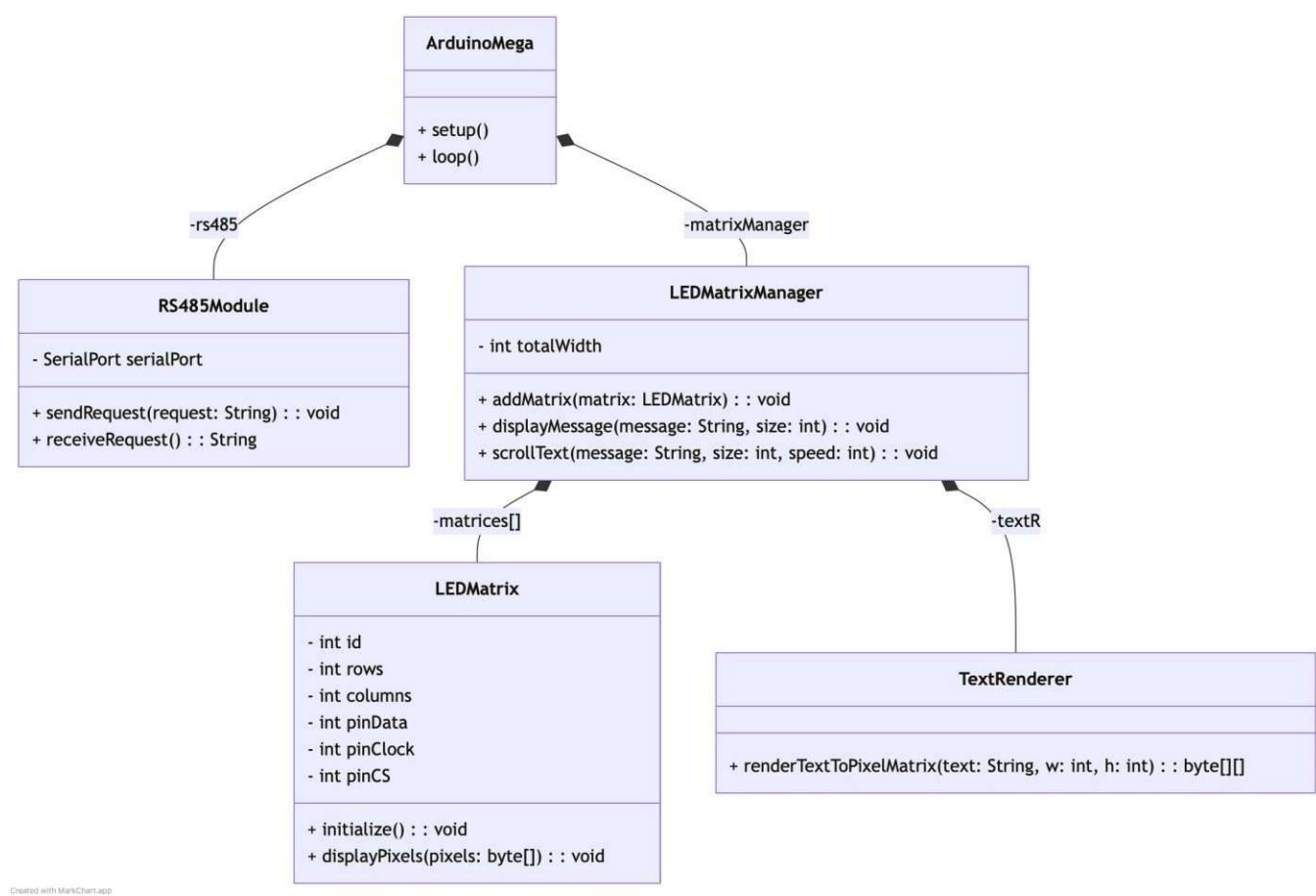
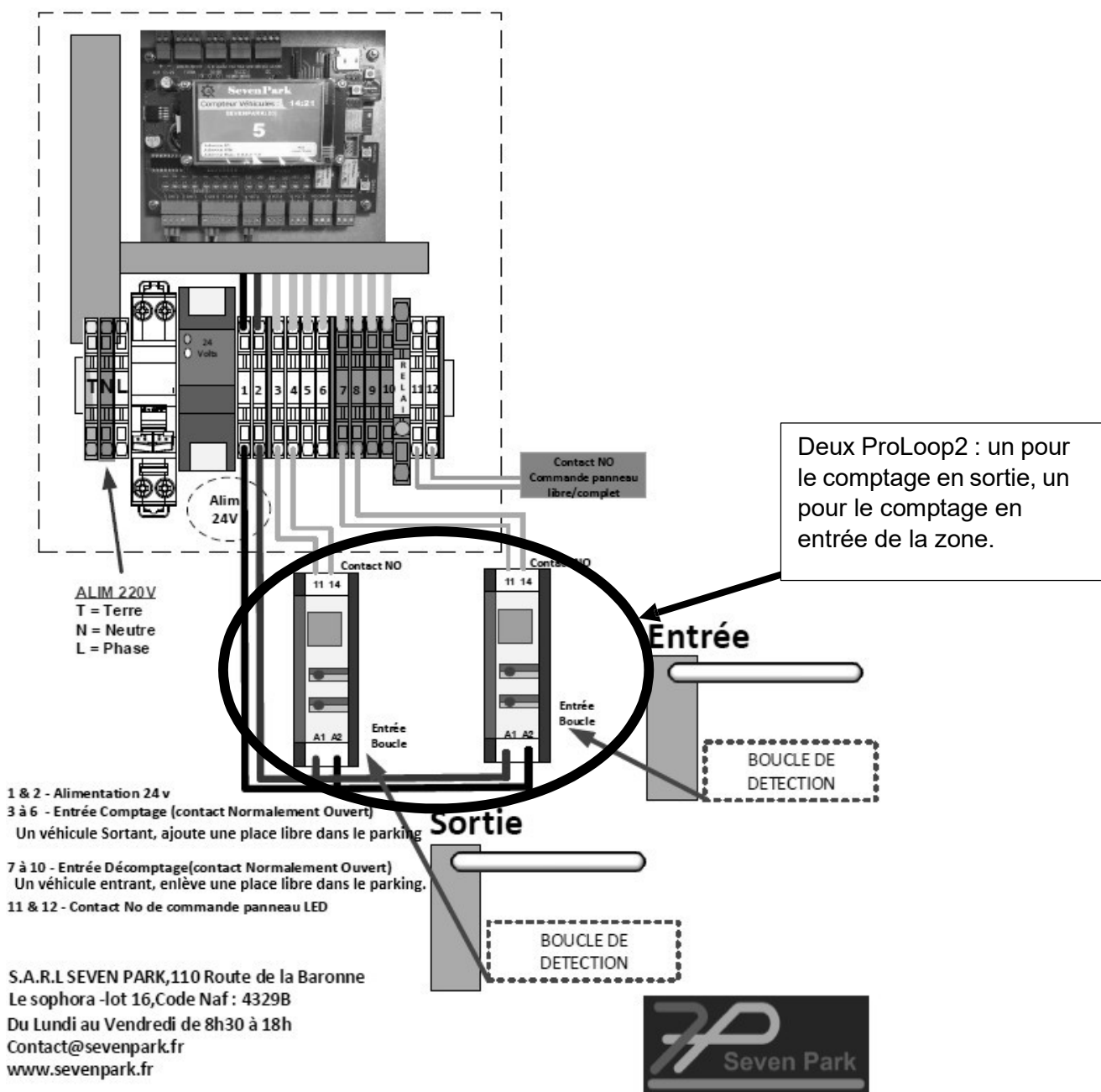


Diagramme de classe simplifié du logiciel d’affichage de l’Arduino Méga

DT14 - Notice d'Installation Système de comptage avec Boucle au Sol (ESP 32)

NOTICE D'INSTALLATION SYSTEME DE COMPTAGE



DT15 - Détecteur de boucle : ProLoop2

ProLoop2

Détecteur de boucle pour portails industriels, barrières automatiques, équipement de parkings et bornes escamotables

Système de détection

Avec ProLoop2, chaque détection de boucle a un fonctionnement absolument sûr. ProLoop2 contrôle et évalue les boucles d'induction enterrées et détecte ainsi tous les types de véhicules de masse métallique: Les vélos, voitures, chariots élévateurs, camions, véhicules avec remorque sont détectés avec précision. La facilité de compréhension des commandes et de l'affichage de ProLoop2 sont particulièrement accessibles et conviviaux. La plus grande fiabilité est garantie par la séparation galvanique entre la boucle et le détecteur.

ProLoop2 – il n'y a pas plus simple

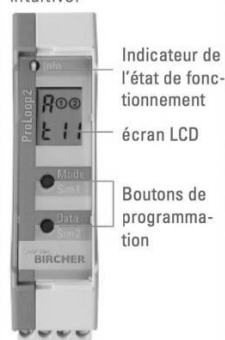
Le programme intelligent et son type de construction permettent une manipulation et une mise en service simples. La version pour embase 11 pôles vous permet de moderniser en adaptant rapidement votre installation de détection à boucle par un simple remplacement de l'appareil.



Vos avantages

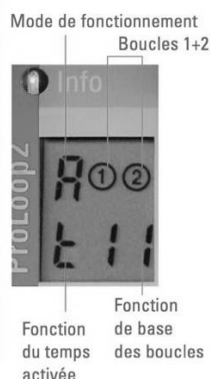
Mise en service rapide

La programmation est rendue facile et simple. Par ses deux boutons et son écran LCD, ProLoop2 s'utilise de manière intuitive.



Facile à utiliser et à superviser

Du premier coup d'oeil sur l'écran LCD de contrôle, vous pouvez lire les états de fonctionnement et les paramètres.



Ajustable individuellement

Ajustage par réglage optimisé de la sensibilité en 9 graduations.



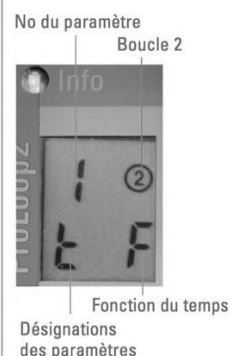
Instrument de mesure intégré

Mesure automatique et affichage de l'inductance en boucle.



Programmable à tout moment

Les fonctions sont facilement ajustables. La temporisation et les autres paramètres sont programmables individuellement.



Sécurité de défaillance secteur

La situation précédant une défaillance secteur est mémorisée en toute sécurité. Après rétablissement de l'alimentation électrique, la valeur réelle relevée est comparée à la valeur mémorisée et les sorties sont activées en fonction de l'occupation de la boucle.



Accessoire supplémentaire

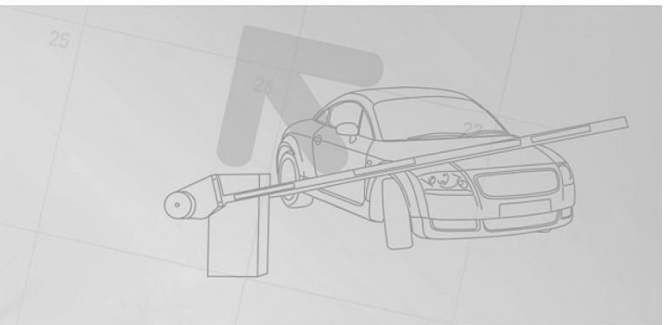
La boucle d'induction préfabriquée est un élément important de la technique sensorielle du détecteur de boucle. Elle est facile à enterrer et est disponible dans différentes dimensions. Des embases (ES 12) pour le ProLoop 11 pôles (rail DIN) sont disponibles.



Embase ES 12 (11 pôles)



Boucle préfabriquée



Applications

Situation

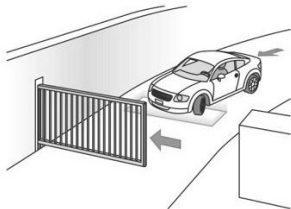
Applications pour portails

Solution

- Ouverture et fermeture de portails en domaine interne et externe

Avantages

- Activation sans contact du portail
- Réagit à tous les véhicules métalliques



Situation

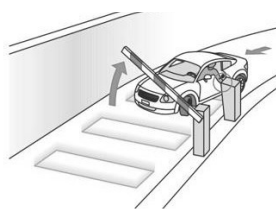
Applications pour barrières levantes

Solution

- Ouverture et fermeture de la barrière au niveau de l'entrée et de la sortie des parkings
- Activation par le distributeur de ticket de stationnement

Avantages

- Pour afficher l'occupation des
 - Cette solution permet de compter des véhicules dans un flux.
 - La barrière et le comptage peuvent être liés.



Situation

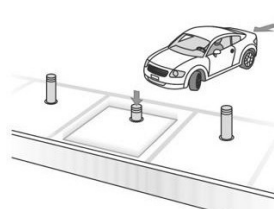
Utilisation avec bornes escamotables

Solution

- Gestion de bornes d'entrée, places de parking, rues et zones piétonnes
- Évite tout déclenchement intempestif des bornes

Avantages

- Pas de risque de collision entre le véhicule et la borne, même après une défaillance secteur



Situation

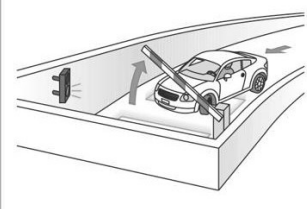
Portails d'entrée avec feux de signalisation

Solution

- Commande de portails et feux de signalisation dans le cas d'accès sans visibilité et de passages exigus

Avantages

- Réglementation routière unique
- Activation ciblée par logique de la circulation
- Temps d'attente réduit par un flux de circulation optimisé

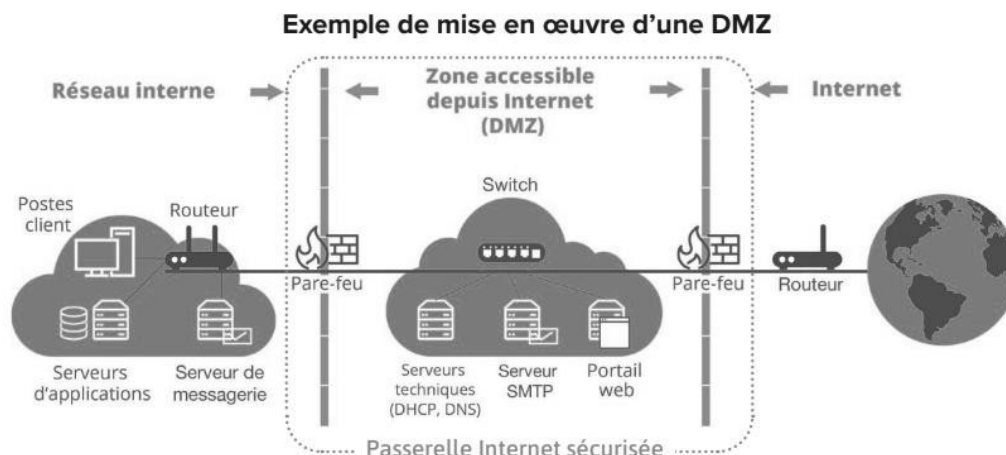


DT16 - Protéger le réseau informatique

Le réseau interne interconnecte l'ensemble des composants des systèmes d'information d'un organisme et dispose souvent de points de connexion avec l'extérieur. Il s'agit tout autant d'un point d'entrée que d'un support de propagation des attaques. Il est donc primordial de sécuriser le réseau interne.

Les précautions élémentaires :

- **limiter les accès Internet** en bloquant les services non nécessaires (VoIP, pair à pair) ;
- **gérer les réseaux Wi-Fi**. Ils doivent utiliser un chiffrement à l'état de l'art (WPA3 ou WPA2 en respectant les recommandations de l'ANSSI sur la configuration de ce dernier) et les réseaux ouverts aux invités doivent être séparés du réseau interne ;
- **imposer un VPN pour l'accès à distance** avec, si possible, une authentification robuste de l'utilisateur (ex. : carte à puce, mot de passe à usage unique basé sur le temps (TOTP)) ;
- **s'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet**. Les opérations d'administration et de maintenance doivent tout particulièrement s'effectuer à travers un VPN ;
- privilégier le protocole SSH (correctement configuré) ou un accès physique direct pour l'administration des équipements réseau ;
- **limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (ex : pare-feux, serveurs proxy). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports ;
- **cloisonner le réseau** pour réduire l'impact en cas de compromission. On peut au minimum distinguer un **réseau interne sur lequel aucune connexion venant d'Internet n'est autorisée** et un **réseau DMZ (« demilitarized zone ») accessible depuis Internet**, en les séparant par des passerelles (« gateway »).



(Source : site web de la CNIL)

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC21 sur 28

DT17 - Rappels et commandes de base sur les commutateurs Cisco

Rappels :

- les commutateurs modernes utilisent des VLAN pour améliorer les performances réseau en divisant les vastes domaines de diffusion de couche 2 en domaines plus petits. Ces VLAN peuvent également être utilisés comme mesure de sécurité en contrôlant quels hôtes peuvent communiquer. D'une manière générale, les VLAN permettent d'adapter un réseau aux objectifs de l'entreprise ;
- les trunks de VLAN sont utilisés pour étendre des VLAN sur plusieurs périphériques. Les trunks permettent au trafic issu de plusieurs VLAN de circuler sur une liaison unique, tout en maintenant intactes l'identification et la segmentation des VLAN. » (Source : Cisco) ;
- les commutateurs Cisco peuvent être configurés avec une adresse IP spéciale appelée interface virtuelle de commutateur (SVI). Le SVI, ou l'adresse de gestion, peut être utilisé pour un accès à distance au commutateur afin d'afficher ou de configurer des paramètres. Si le SVI du VLAN 1 est attribué à une adresse IP, tous les ports dans le VLAN 1 disposent d'un accès par défaut à l'adresse IP du SVI. (Source : Cisco)

Commandes de base :

DÉFINIR et NOMMER un nouveau VLAN :

```
# Définir le VLAN 10 (Admin)
switch(conf)# vlan 10
switch(conf-vlan)# name Admin
switch(conf-vlan)# exit
```

RATTACHER UN PORT à un VLAN :

```
# Rattacher le port fa0/1 au vlan 10
switch(conf)# interface fa0/1
switch(conf-if)# switchport mode access
switch(conf-if)# switchport access vlan 10
switch(conf-if)# exit
```

RATTACHER UN ensemble de PORTS à un VLAN :

```
# Rattacher le port fa0/5 à fa0/10 (donc 6 ports au total) au vlan 10
switch(conf)# interface range fa0/5 – 10
switch(conf-if-range)# switchport mode access
switch(conf-if-range)# switchport access vlan 10
switch(conf-if-range)# exit
```

CONFIGURER UN PORT en mode TRUNK :

```
# Configurer le port fa0/24 en mode trunk
switch(conf)# interface fa0/24
switch(conf-if)# switchport mode trunk
switch(conf-if)# exit
```

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC22 sur 28

CONFIGURER L'INTERFACE D'ADMINISTRATION SUR LE VLAN 2 :

```
# Configurer le VLAN d'administration du switch sur vlan 2
switch(conf)# interface vlan 2
switch(conf-if)# ip address 192.168.100.254 255.255.255.0
switch(conf-if)# exit
```

AFFICHER TOUTE LA CONFIGURATION ACTUELLE :

```
# afficher la configuration courante
switch# show running-config
```

AFFICHER LES INFORMATIONS SUR LES VLAN ET AFFECTATION DES PORTS :

```
# afficher les vlan définis et l'affectation des ports dans les vlan
switch(conf)# show vlan
```

AFFICHER LES INFORMATIONS SUR LA CONFIGURATION IP DES INTERFACES :

```
# Configurer le VLAN d'administration du switch sur vlan 2
switch(conf)# show ip interface brief
```

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC23 sur 28

DT18 - Le RGPD, qu'est-ce que c'est ?

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018.

Il a été conçu autour de trois objectifs :

- **renforcer les droits des personnes** ;
- **responsabiliser les acteurs traitant des données** ;
- **crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données.

Données personnelles : de quoi parle-t-on ?

Une **donnée à caractère personnel** (ou « **donnée personnelle** ») est décrite par la Commission nationale de l'informatique et des libertés (CNIL) comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il existe deux types d'identification :

- **identification directe** (nom, prénom, etc.) ;
- **identification indirecte** (identifiant, numéro, etc.).

Lorsqu'une opération ou un ensemble d'opérations portant sur des données personnelles sont effectuées, on considère qu'il s'agit de **traitement de données personnelles**.

Êtes-vous concerné par le RGPD ?

Le RGPD s'adresse à toute structure privée ou publique effectuant de la collecte et/ou du traitement de données, et ce quel que soit son secteur d'activité et sa taille. Le règlement s'applique à **tous les organismes établis sur le territoire de l'Union européenne**, mais aussi à tout organisme implanté hors de l'UE mais dont l'activité cible directement des résidents européens.

Ainsi, si vous collectez et/ou traitez des données personnelles, vous avez des obligations vis-à-vis de l'internaute.

Utilisation de données personnelles : vos obligations vis-à-vis de l'internaute.

Le **RGPD** stipule trois moments où vous devez informer l'internaute :

1. vous devez informer l'internaute **au moment de la collecte de ses données personnelles** dans le cas d'une collecte directe ou dès que possible dans le cas d'une collecte indirecte de données (lors du premier contact par exemple) ;
2. vous devez également informer l'internaute de l'utilisation de ses données **en cas de modification de leur utilisation** ;
3. enfin, dans un souci de transparence, vous devez informer **régulièrement** l'internaute de l'utilisation de ses données personnelles.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC24 sur 28

Utilisation de données personnelles : quelles informations donner à l'internaute ?

Le **RGPD** précise les informations que vous devez rendre disponibles. Ainsi, si un internaute vous en fait la demande, vous avez l'obligation de donner accès aux informations suivantes :

- identité et coordonnées de l'organisme responsable du traitement de données ;
- coordonnées du délégué à la protection des données (DPO) ou d'un point de contact sur les questions de protection des données personnelles ;
- base juridique du traitement de données (consentement de l'internaute, respect d'une obligation prévue par un texte, exécution d'un contrat...) ;
- **finalités des données collectées** (pour prise de décision automatisée, pour prévenir la fraude, parce que les informations sont requises par la réglementation...) ;
- caractère obligatoire ou facultatif du recueil des données et les conséquences pour la personne en cas de non-fourniture des données ;
- destinataires ou catégories de destinataires des données ;
- **durée de conservation** des données ;
- transferts de données à caractère personnel envisagés à destination d'un État n'appartenant pas à l'Union européenne.

Vous devez également **informer l'internaute de ses droits** : accès à ses données, possibilité de rectification ou d'effacement de ses données, de retrait de son consentement, possibilité de faire une réclamation auprès de la CNIL.

En cas de données collectées de manière indirecte, vous devez informer l'internaute de la source des données.

Source : <https://www.economie.gouv.fr/>

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC25 sur 28

DT19 - Documentation commande mysqldump

Source : wikipédia

Mysqldump peut sauvegarder des bases de données MySQL. Son fonctionnement est particulièrement intéressant car elle génère les commandes SQL permettant de recréer la base de données sur un autre serveur, ou d'exporter les données vers du CSV et du XML.

Backup

Pour exporter la base de données « myBase », on utilise la commande suivante :

```
mysqldump -u root -p myBase > myBase_backup.sql (syntaxe 1)
```

Ceci fera l'export dans un fichier « myBase_backup.sql ».

Exemple de dump d'une base :

```
mysqldump --user=root --password=mon_mdp ma_base > my_base.sql (syntaxe 2)
```

Pour dumper toutes les bases :

```
mysqldump --user=root --password=mon_mdp --all-databases > all_db.sql
```

Pour dumper certains enregistrements de certaines tables :

```
mysqldump --database ma_base --tables ma_table --where="id in (1, 2, 3)" --  
user=root --password=mon_mdp > my_query.sql
```

Sans les données

Pour ne récupérer que le schéma :

```
Mysqldump -f --no-data --user=root --password=mon_mdp ma_base > my_base_schema.sql
```

Tâche planifiée

Pour définir le backup automatique d'une base tous les soirs à minuit, sous Linux :

```
$ crontab -e  
  
0 0 * * * /usr/local/bin/mysqldump -uLOGIN -PPORT -hHOST -pPASS base1 | gzip  
-c > `date "+\%Y-\%m-\%d"` .gz
```

Le fichier décompresser est au format SQL et peut donc être exécuter pour recréer les bases, tables, et insérer les enregistrements.

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC26 sur 28

DT20 - Documentation sur fichier « crontab »

Syntaxe d'un fichier **crontab** :

```
# * * * * * command to be executed
```

Le fichier est constitué de différentes lignes. Chaque ligne correspond à une commande à exécuter.

Prenons l'exemple suivant : `mm hh jj MMM JJJ tâche >> log`

- `mm` : minutes (00-59).
- `hh` : heures (00-23) .
- `jj` : jour du mois (01-31).
- `MMM` : mois (01-12 ou abréviation anglaise sur trois lettres : jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec).
- `JJJ` : jour de la semaine (1-7 ou abréviation anglaise sur trois lettres : mon, tue, wed, thu, fri, sat, sun).
- `tâche` : commande à exécuter.
- `>> log` (facultatif) : redirection de la sortie vers un fichier de log. Si un fichier de log n'est pas spécifié, un mail sera envoyé à l'utilisateur local.
- Pour chaque unité, on peut utiliser les notations suivantes :
 - 1-5 : les unités de temps de 1 à 5.
 - */6 : toutes les 6 unités de temps (toutes les 6 heures par exemple).
 - 2, 7 : les unités de temps 2 et 7.

Exemples :

Exécution tous les jours à 22 h 00 d'une commande et rediriger les infos dans sauvegarde.log :

```
00 22 * * * /root/scripts/sauvegarde.sh >> sauvegarde.log
```

Exécution d'une commande toutes les 6 heures :

```
00 */6 * * * /root/scripts/synchronisation-ftp.sh
```

Exécution d'une commande toutes les 6 minutes :

```
*/6 * * * * /root/scripts/synchronisation-ftp.sh
```

Exécution d'une commande toutes les minutes uniquement les lundis :

```
* * * * 1 /root/scripts/commandes-du-lundi.sh
```

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC27 sur 28

DT21 - Réponse d'un « chatbot » à une question sur la réplication du SGBDR MariaDB

La réplication de base de données MariaDB

La réplication de base de données est un processus qui permet de copier les données d'une base de données principale (master) vers une ou plusieurs bases de données secondaires (esclaves ou réplicas). Cette fonctionnalité est essentielle pour assurer la haute disponibilité, la redondance des données et équilibrer la charge de travail.

Comment fonctionne la réplication de MariaDB ?

La réplication de MariaDB utilise une configuration maître-esclave. Le serveur maître active le binlog, qui enregistre toutes les modifications apportées aux données (mises à jour, insertions, suppressions). Les serveurs esclaves lisent ensuite le binlog du maître et appliquent ces mêmes modifications sur leurs propres bases de données.

Comment configurer la réplication de MariaDB ?

Voici les étapes générales pour configurer la réplication de MariaDB :

- **préparer le serveur maître** : activer le binlog, créer un utilisateur de réplication et configurer le `server_id` ;
- **configurer les serveurs esclaves** : désigner le serveur maître, configurer le `server_id` et démarrer la réplication ;
- **vérifier l'état de la réplication** : utiliser la commande `SHOW SLAVE STATUS`, pour s'assurer que la réplication fonctionne correctement.

Quels sont les avantages de la réplication de MariaDB ?

- **haute disponibilité** : Si le serveur maître tombe en panne, vous pouvez rapidement basculer vers un serveur esclave ;
- **redondance des données** : Les données sont répliquées sur plusieurs serveurs, ce qui les protège contre les pertes ;
- **équilibrage de charge** : Les requêtes de lecture peuvent être réparties sur les serveurs esclaves, allégeant la charge sur le maître.

En conclusion, la réplication de MariaDB est une fonctionnalité cruciale pour les environnements de production exigeants, offrant une meilleure fiabilité, redondance et performance.

Sources :

MySQL Replication Master | MariaDB Knowledge Base
Réplicas en lecture d'Amazon RDS | Service de base de données
MariaDB Replication : Easy Methods | Hevo
JSON Data Type – MariaDB Knowledge Base
MariaDB Replication – MariaDB Knowledge Base

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE OPTION INFORMATIQUE ET RÉSEAUX		Session 2025
Étude et conception de réseaux informatiques – E4	Code : 25CIELAECRI	Page DOC28 sur 28