

Note	Compétences	Acquise	Non Acquise
	<b>C04</b> : Analyser un système informatique		
/20	<b>C05</b> : Concevoir un système informatique		

## Semaine n°2 - Mission n°1

### Analyser les trames du protocole CIP et Modbus RTU

#### FICHE MISSION 1

##### Premier Audit de Sécurité et Analyse de Trames

**I – PROBLEMATIQUE** : Comment analyser la sécurité d'un système industriel ?

**II – OBJECTIFS** :

- Analyser les trames du protocole **CIP**
- Analyser les trames du protocole **Modbus RTU**

**III – PRE-REQUIS** :

- Etre à l'aise avec la lecture des diagrammes **SysML** et **UML**
- Connaître les principes de base de la cybersécurité (gestion des mots de passe, principe du moindre privilège, .....)

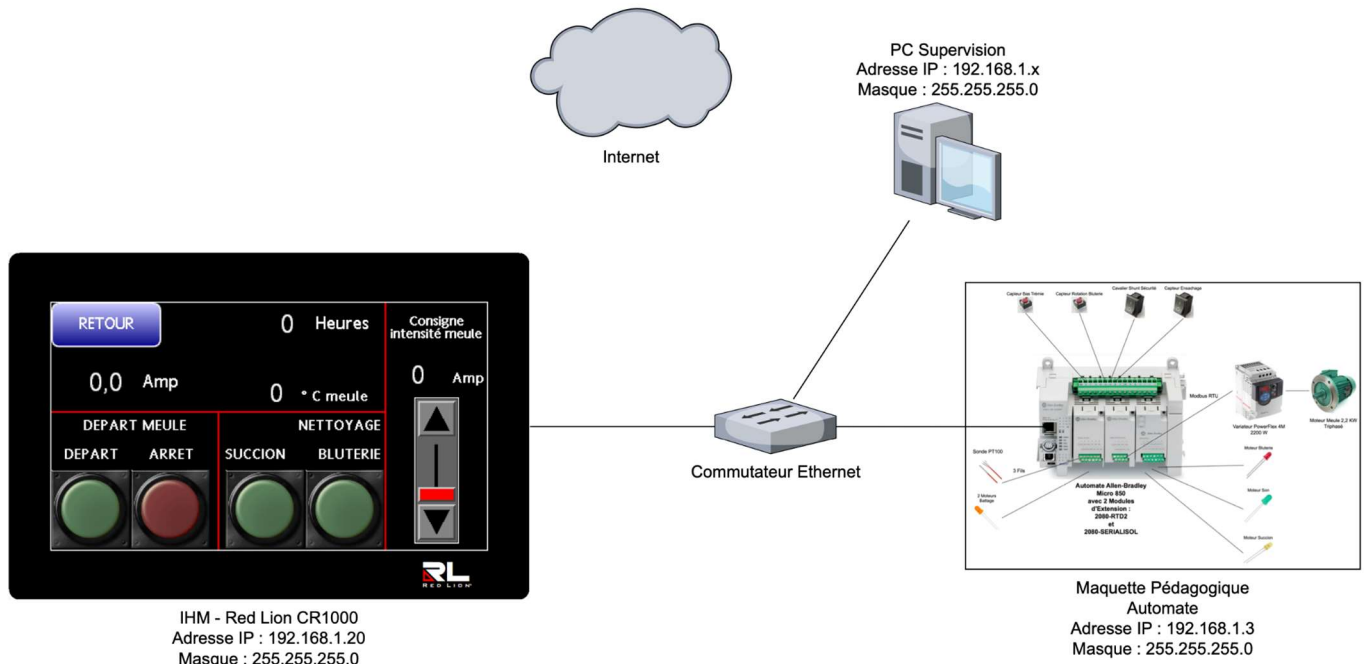
**IV – MISE EN SITUATION** : Lors de la semaine précédente, vous avez étudié le système, pris en main la maquette pédagogique et planifié le déploiement d'un système de supervision. Dans cette mission, nous allons analyser les protocoles industriels utilisés sur le système.

**V – RESSOURCES MATERIELLES** : Vous réaliserez cette mission en travaillant avec un **PC** connecté à **Internet** et un accès à un environnement de travail de type **Workspace** avec les outils bureautique :

- Traitement de texte.
- Tableur.
- Logiciel de diaporama.
- Logiciel **Connect Components Workbench (CCW)** avec le programme de l'automate fourni.
- Logiciel **Crimson** avec le programme de l'IHM fourni.
- Logiciel de décodage de trames.
- Convertisseur **USB Modbus RTU**.

**VI – RESSOURCES PEDAGOGIQUES** : Vous utiliserez le dossier technique fourni ainsi que la documentation technique du variateur **Powerflex** et du protocole **Modbus RTU**.

## VII – SCHEMA DU RESEAU :



L'enseignant vous fournira votre Adresse IP au début de la séance

## VIII – ACTIVATION DU WEB SERVER ET PREMIER AUDIT DE SECURITE :

Nous allons nous intéresser à la communication entre l'automate et l'IHM. Pour réaliser ceci, vous allez devoir activer le **Web Server** sur l'IHM. Il faut réaliser cette configuration depuis le logiciel **Crimson**.

Donner la procédure pour réaliser ceci.

.....

Accéder au **Web Server** de l'IHM. Quel est le mot de passe par défaut de l'IHM sur l'interface du **Web Server** ? Ce mot de passe est-il complexe ?

.....

Noter dans un fichier les préconisations d'évolution à proposer en termes de sécurité. Commencer par : **Préconisation n°1** : Mot de passe faible de l'accès au **Web Server** de l'IHM.

Naviguer dans les menus du Web Server et identifier trois autres préconisations de sécurité.

.....

### IX – ANALYSE DE TRAMES DU PROTOCOLE CIP :

Lancer une capture de trames depuis le **Web Server**. Exporter cette capture de trames sur votre ordinateur et ouvrir cette capture de trames avec **Wireshark**.

Décrire les étapes pour réaliser ceci.

.....

.....

Analyser cette trame. Quel protocole de communication voyez-vous entre l'automate et l'**IHM** ? Ce protocole est-il sécurisé ?

.....

.....

Réaliser la même opération, capturer une trame de communication mais en la réalisant directement depuis votre poste client. Pour cela, lancer l'émulateur de l'**IHM** dans le programme **Crimson** et capturer des trames depuis **Wireshark**.

Décrire les étapes pour réaliser ceci.

.....

.....

Analyser cette trame. Quel protocole de communication voyez-vous entre l'automate et l'**IHM** ? Ce protocole est-il toujours sécurisé ?

.....

.....

Quel protocole de communication voyez-vous entre le poste client et l'**IHM** concernant l'accès au **Web Server** ? Ce protocole est-il sécurisé ?

.....

.....

Conclure sur la sécurité des échanges de communication entre l'automate et l'**IHM** et entre le poste client et l'**IHM**.

.....

.....

### X – ANALYSE DE TRAMES DU PROTOCOLE MODBUS RTU :

Nous allons maintenant réaliser une capture de trames du protocole **Modbus RTU**. Vous ferez cette capture de trames en présence de votre enseignant car vous allez devoir câbler quelques fils sur l'automate.

Décrire les étapes pour réaliser une capture de trames du protocole **Modbus RTU** en présence de votre enseignant.

.....

.....

Vous allez maintenant analyser les trames relevées. A l'aide de la documentation technique du variateur **Powerflex** et du protocole **Modbus RTU**, essayer de retrouver par le calcul la valeur du courant de la meule mesurée et la valeur de la fréquence de fonctionnement du moteur.

.....

.....

Conclure sur la sécurité du protocole **Modbus RTU**.

.....

.....

#### **XI – PISTE DE REFLEXION SUR LA SECURISATION DU SYSTEME :**

Donner des pistes d'amélioration pour sécuriser le protocole **CIP** et le protocole **Modbus RTU**. Les modèles de l'automate et de l'**IHM** peuvent-ils être sécurisés ?

.....

.....

Sur quels éléments de configuration peut-on agir pour sécuriser le système ?

.....

.....

Quels ajouts d'équipements doivent être envisagés pour réduire les risques de piratage industriel ?

.....

.....

Grille de Notation

Validation Compétences

Web Server activée		/2	
Premier audit de sécurité réalisé		/4	
Protocole <b>CIP</b> analysé		/4	
Protocole <b>Modbus RTU</b> analysé		/4	Valide C04
Pistes de sécurité envisagées		/6	Valide C05
Barème de notation total		/20	

## Correction

### Etude des échanges entre l'automate et l'IHM

Nous allons tout d'abord étudier les échanges entre l'automate et l'IHM. Voici le schéma réseau que nous utiliserons pour notre laboratoire de test :

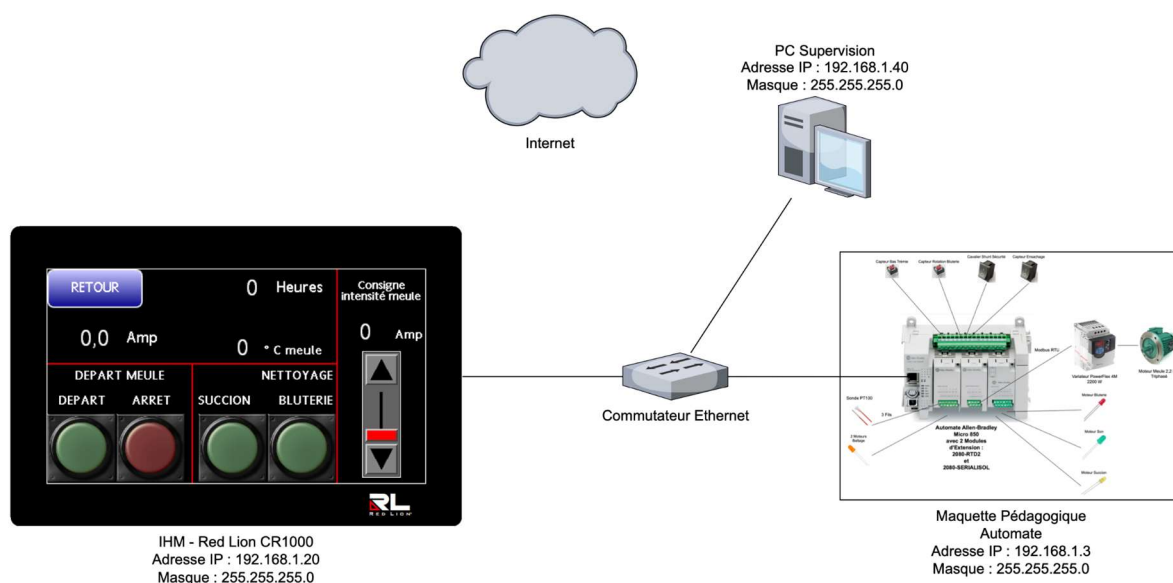


Fig. 5 - Schéma réseau pour le laboratoire de test (Lab)

Nous avons volontairement fait le choix de ne pas relier le réseau à Internet, nous reviendrons sur ce point plus tard.

Pour réaliser la capture de trames, nous allons procéder de deux façons différentes :

- Méthode n°1 : Capturer des trames depuis l'IHM.
- Méthode n°2 : Capturer des trames depuis le **PC Supervision**.

Méthode n°1 : Capturer des trames depuis l'IHM

Pour capturer les trames sur l'IHM, il faut activer le **Web Server** sur celui-ci :

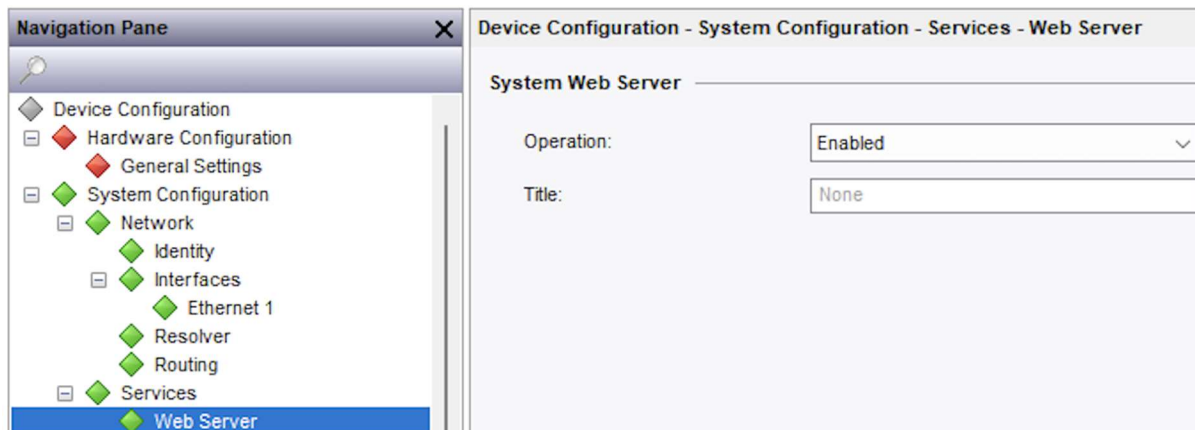
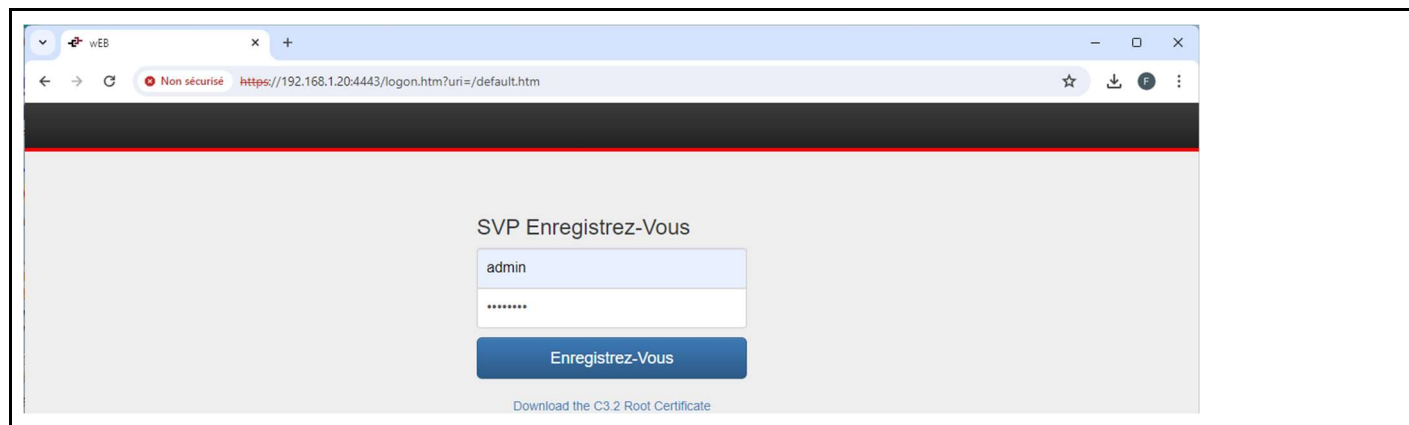


Fig. 6 - Configuration du Web Server sur l'IHM

Nous pouvons donc maintenant accéder à un **serveur Web**, avoir des informations générales sur l'IHM et accéder à une interface de capture des trames :



The screenshot displays the web interface of a CR1000-04000 device. The top navigation bar includes links for 'Retour', 'Configuration', 'Diagnostics', and 'Help', along with the device ID 'CR1000-04000 06-98-6B' and the user 'Administrator'.

### WEB

#### Device Information

Device Model	CR1000-04000
Enabled Group	Group 3 (Full Crimson Functionality)
Serial Number	06-98-6B
Software Version	3.2.1016.0

#### Crimson Runtime

Status: Running

[Stop System](#) [Start System](#)

#### Interface Status

Interface	Device	Status	IP Address	Network Mask	MAC Address	Connection
Ethernet 1	eth0	UP	192.168.1.20	255.255.255.0	00:05:E4:06:98:6B	100M, Full Duplex

#### Quick Access

[Configuration](#) [Diagnostics](#) [Network Capture](#) [System Info](#)

Capture Source: Ethernet 1

Quick Enable: [All Traffic](#) [All Non-Web](#)

TCP Capture: [All Traffic](#) TCP Port:

UDP Capture: [Disabled](#) UDP Port:

ICMP Capture: [Disabled](#)

Management Frames: [Disabled](#)

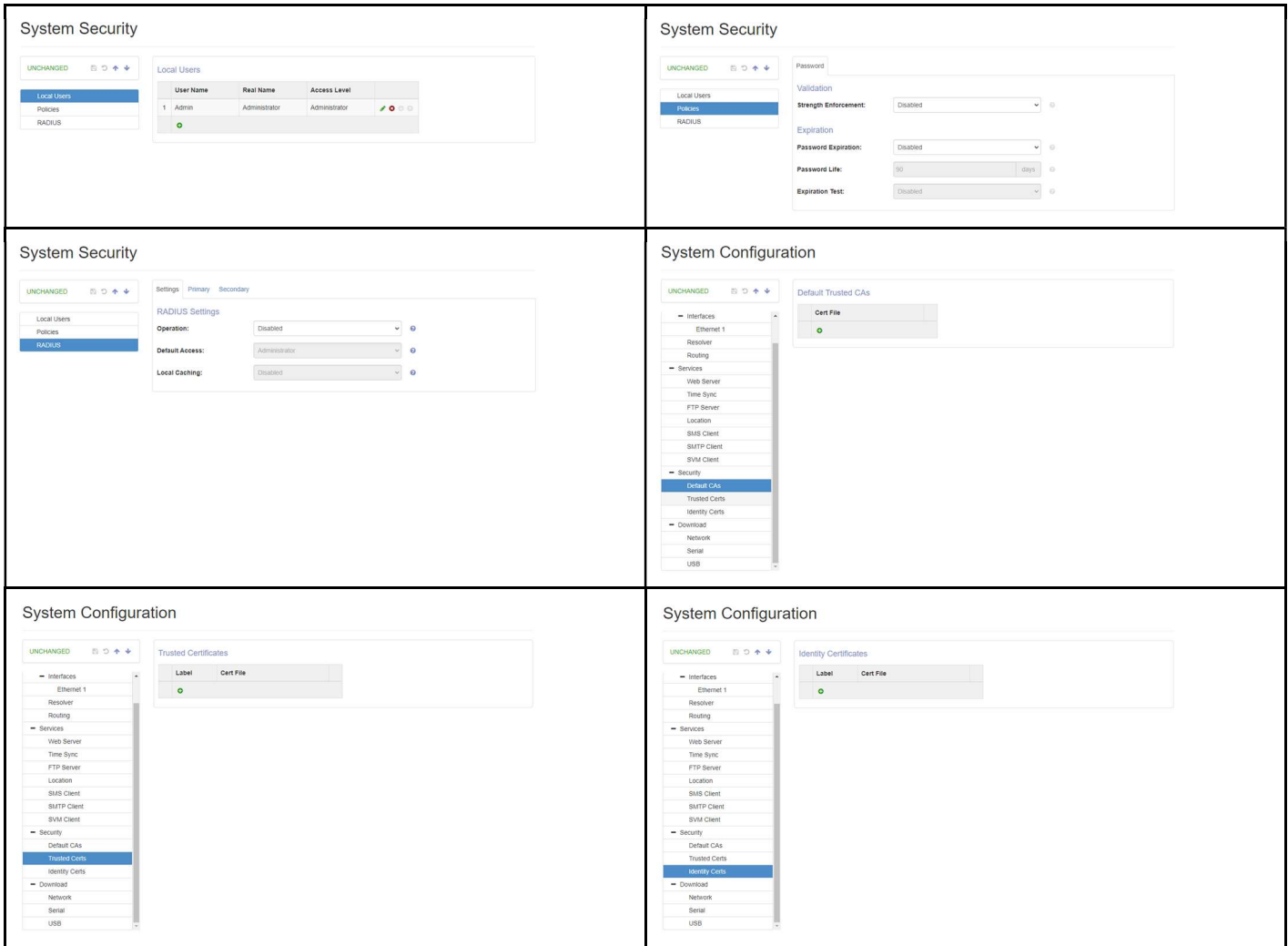
[Start Capture](#)

[Download the network capture.](#)  
262210 bytes available.

Fig. 7 - Accès au Web Server et à la capture de trames

En accédant aux différents paramètres de l'IHM, plusieurs points de vigilance sont à mettre en évidence :

1. Le login de l'IHM par défaut est **admin** et le mot de passe est **password**, il faut absolument le mettre à jour avec un mot de passe sécurisé et surtout créer des utilisateurs avec des droits spécifiques, principe fondamental du moindre privilège. Il est possible d'utiliser une authentification **RADIUS**, piste sérieuse à creuser si l'entreprise décide de gérer l'intégralité de ces moulins à distance.
2. La fonction d'utilisation des mots de passe complexe (**Strenght Enforcement**) est désactivée et la durée de vie des mots de passe (**Password Expiration**) est également désactivée.
3. Aucune autorité de certification n'a été configurée, aucun certificat et aucune clé n'ont été installés.



*Fig. 8 - Mise en évidence des problèmes de sécurité*

4. Aucun filtrage d'adresse IP n'est réalisé : IP Filter → Permitted Address (0.0.0.0) et Permitted Mask : 0.0.0.0.



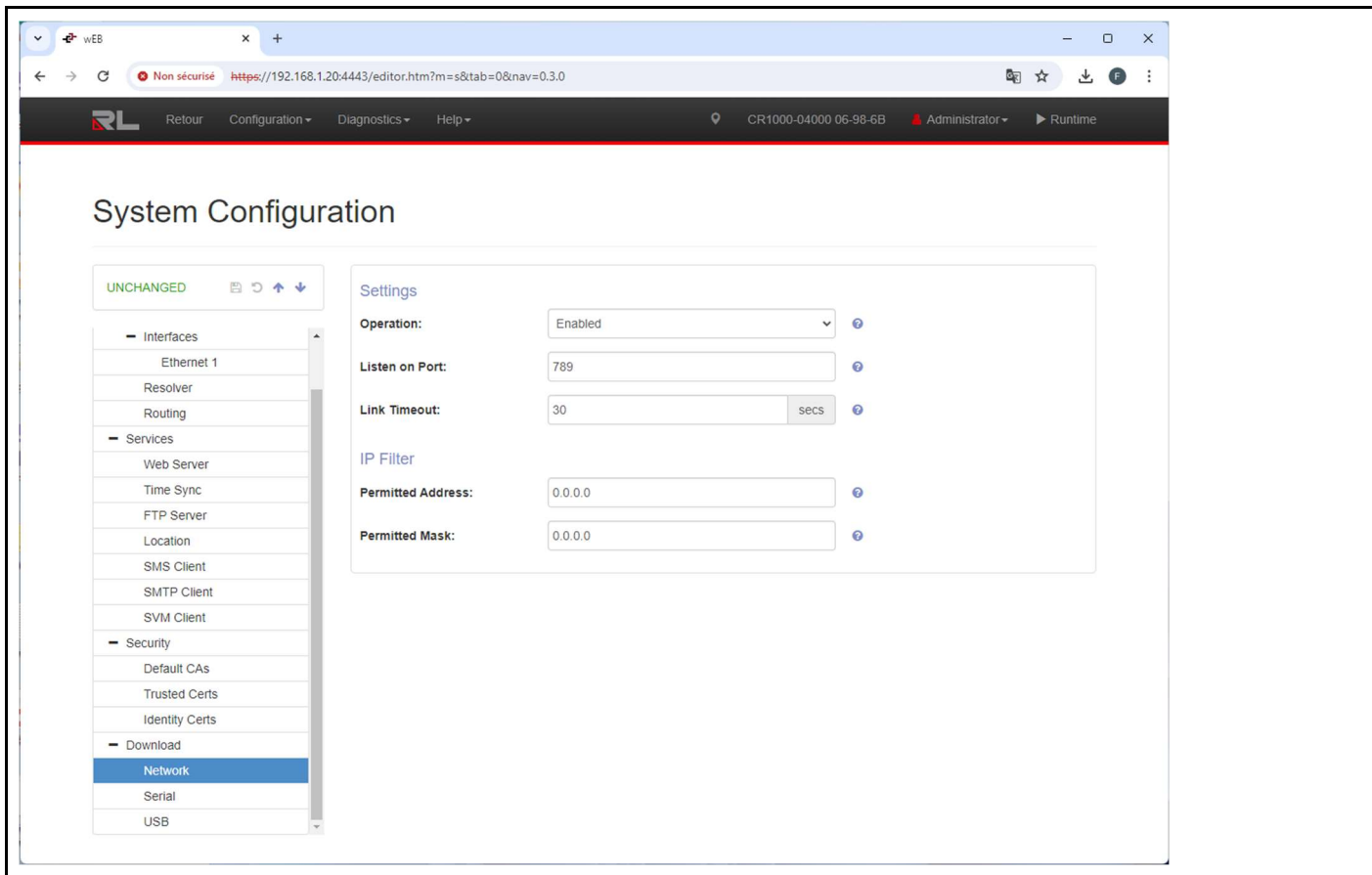


Fig. 9 - Mise en évidence des problèmes de filtrage d'adresse IP

Nous allons effectuer plusieurs manipulations concernant le fonctionnement du système et vous trouverez l'ensemble des captures de trames réalisées dans le sous-dossier **Crimson** du Drive Partagé :

### Crimson

Les deux captures de trame suivantes mettent en évidence 2 phénomènes :

- La première capture de trame correspond à une capture réalisée depuis le **PC Supervision** qui accède à l'interface Web du **Web Server** en utilisant un navigateur Internet. Nous pouvons visualiser que les échanges sont cryptés (**TLS v1.3**) bien qu'il n'y ait aucune autorité de certification autorisée dans la configuration de l'IHM, ce qui est déjà un bon point. Nous pouvons justifier cela par un avertissement au lancement du **Web Server**, en effet, il utilise un certificat auto-signé, ce qui n'est pas recommandé par l'ANSSI.
- La deuxième capture de trames est réalisée sur le **Web Server** de l'IHM est un export du fichier **.pcpng** vers **Wireshark** pour le décoder. Nous avons simulé une alarme bluterie et nous visualisons toutes les variables en clair mais aussi les opérations de commandes des différents organes du système !

13	11.651847	192.168.1.40	192.168.1.20	TCP	66	51658 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
14	11.653167	192.168.1.20	192.168.1.40	TCP	60	4443 → 51658 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1280
15	11.653218	192.168.1.40	192.168.1.20	TCP	54	51658 → 4443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	11.653679	192.168.1.40	192.168.1.20	TCP	1334	51658 → 4443 [ACK] Seq=1 Ack=1 Win=64240 Len=1280 [TCP segment of a reassembled PDU]
17	11.661731	192.168.1.20	192.168.1.40	TCP	60	4443 → 51658 [ACK] Seq=1 Ack=1281 Win=1460 Len=0
18	11.661755	192.168.1.40	192.168.1.20	TLV1.3	539	Client Hello
19	11.672120	192.168.1.20	192.168.1.40	TLV1.3	185	Hello Retry Request
20	11.672951	192.168.1.40	192.168.1.20	TLV1.3	671	Change Cipher Spec, Client Hello
21	11.776336	192.168.1.20	192.168.1.40	TCP	60	4443 → 51658 [ACK] Seq=132 Ack=2383 Win=1460 Len=0
22	11.968657	192.168.1.20	192.168.1.40	TLV1.3	1334	Server Hello, Application Data
23	11.969882	192.168.1.20	192.168.1.40	TLV1.3	1334	Application Data, Application Data
24	11.969882	192.168.1.20	192.168.1.40	TLV1.3	97	Application Data
25	11.969971	192.168.1.40	192.168.1.20	TCP	54	51658 → 4443 [ACK] Seq=2383 Ack=2735 Win=65280 Len=0
26	11.970481	192.168.1.40	192.168.1.20	TLV1.3	78	Application Data
27	11.970769	192.168.1.40	192.168.1.20	TCP	54	51658 → 4443 [FIN, ACK] Seq=2407 Ack=2735 Win=65280 Len=0
28	11.971169	192.168.1.20	192.168.1.40	TCP	60	4443 → 51658 [ACK] Seq=2735 Ack=2408 Win=1460 Len=0
29	11.972544	192.168.1.40	192.168.1.20	TCP	66	51659 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
30	11.973563	192.168.1.20	192.168.1.40	TCP	60	4443 → 51659 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1280
31	11.973718	192.168.1.40	192.168.1.20	TCP	54	51659 → 4443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
32	11.975580	192.168.1.40	192.168.1.20	TCP	1334	51659 → 4443 [ACK] Seq=1 Ack=1 Win=64240 Len=1280 [TCP segment of a reassembled PDU]
33	11.977267	192.168.1.20	192.168.1.40	TCP	60	4443 → 51658 [RST] Seq=2735 Win=0 Len=0
34	11.977315	192.168.1.20	192.168.1.40	TCP	60	4443 → 51659 [ACK] Seq=1 Ack=1281 Win=1460 Len=0

Fig. 10 - Capture de trames de l'accès au Web Server en HTTPS

2	0.005000	192.168.1.20	192.168.1.3	CIP	118	'start_poxerflex' - Service (0x4c)
3	0.005000	192.168.1.3	192.168.1.20	CIP	101	Success: 'start_poxerflex' - Service (0x4c)
4	0.015000	192.168.1.20	192.168.1.3	CIP	116	'capt_rot_blut' - Service (0x4c)
5	0.015000	192.168.1.3	192.168.1.20	CIP	101	Success: 'capt_rot_blut' - Service (0x4c)
6	0.025000	192.168.1.20	192.168.1.3	CIP	114	'alarm_entret' - Service (0x4c)
7	0.025000	192.168.1.3	192.168.1.20	CIP	101	Success: 'alarm_entret' - Service (0x4c)
8	0.035000	192.168.1.20	192.168.1.3	CIP	118	'intense_meule' - Service (0x4c)
9	0.035000	192.168.1.3	192.168.1.20	CIP	101	Success: 'intense_meule' - Service (0x4c)
10	0.045000	192.168.1.20	192.168.1.3	CIP	112	'activ_rend' - Service (0x4c)
11	0.045000	192.168.1.3	192.168.1.20	CIP	101	Success: 'activ_rend' - Service (0x4c)
12	0.050000	192.168.1.40	192.168.1.20	TCP	60	51596 → 4443 [ACK] Seq=1 Ack=129 Win=65152 Len=0
13	0.055000	192.168.1.20	192.168.1.3	CIP	114	'arret_vibra' - Service (0x4c)
14	0.055000	192.168.1.3	192.168.1.20	CIP	101	Success: 'arret_vibra' - Service (0x4c)
15	0.065000	192.168.1.20	192.168.1.3	CIP	114	'vibra_eleve' - Service (0x4c)
16	0.065000	192.168.1.3	192.168.1.20	CIP	101	Success: 'vibra_eleve' - Service (0x4c)
17	0.075000	192.168.1.20	192.168.1.3	CIP	116	'succion_force' - Service (0x4c)
18	0.075000	192.168.1.3	192.168.1.20	CIP	101	Success: 'succion_force' - Service (0x4c)
19	0.085000	192.168.1.20	192.168.1.3	CIP	112	'HORAMETRE' - Service (0x4c)
20	0.085000	192.168.1.3	192.168.1.20	CIP	104	Success: 'HORAMETRE' - Service (0x4c)
21	0.095000	192.168.1.20	192.168.1.3	CIP	110	'T_meule' - Service (0x4c)
22	0.095000	192.168.1.3	192.168.1.20	CIP	102	Success: 'T_meule' - Service (0x4c)
23	0.105000	192.168.1.20	192.168.1.3	CIP	116	'current_meule' - Service (0x4c)

Fig. 11 - Capture de trames réalisées sur l'IHM avec l'alarme bluterie

## Méthode n°2 : Capturer des trames depuis le PC Supervision en utilisant l'émulateur

1	0.000000	192.168.1.20	192.168.1.3	CIP	114	'arret_vibra' - Service (0x4c)
2	0.000013	192.168.1.20	192.168.1.3	TCP	114	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=1 Ack=1 Win=1460 Len=60
3	0.003930	192.168.1.3	192.168.1.20	CIP	101	Success: 'arret_vibra' - Service (0x4c)
4	0.037360	192.168.1.20	192.168.1.3	CIP	114	'vibra_eleve' - Service (0x4c)
5	0.037389	192.168.1.20	192.168.1.3	TCP	114	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=61 Ack=48 Win=1460 Len=60
6	0.042936	192.168.1.3	192.168.1.20	CIP	101	Success: 'vibra_eleve' - Service (0x4c)
7	0.091979	192.168.1.20	192.168.1.3	CIP	116	'succion_force' - Service (0x4c)
8	0.092010	192.168.1.20	192.168.1.3	TCP	116	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=121 Ack=95 Win=1460 Len=62
9	0.095470	192.168.1.3	192.168.1.20	CIP	101	Success: 'succion_force' - Service (0x4c)
10	0.139521	192.168.1.20	192.168.1.3	CIP	112	'HORAMETRE' - Service (0x4c)
11	0.139552	192.168.1.20	192.168.1.3	TCP	112	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=183 Ack=142 Win=1460 Len=58
12	0.144144	192.168.1.3	192.168.1.20	CIP	104	Success: 'HORAMETRE' - Service (0x4c)
13	0.171113	192.168.1.20	192.168.1.3	CIP	110	'T_meule' - Service (0x4c)
14	0.171142	192.168.1.20	192.168.1.3	TCP	110	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=241 Ack=192 Win=1460 Len=56
15	0.176424	192.168.1.3	192.168.1.20	CIP	102	Success: 'T_meule' - Service (0x4c)
16	0.218746	192.168.1.20	192.168.1.3	CIP	116	'current_meule' - Service (0x4c)
17	0.218775	192.168.1.20	192.168.1.3	TCP	116	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=297 Ack=240 Win=1460 Len=62
18	0.222871	192.168.1.3	192.168.1.20	CIP	104	Success: 'current_meule' - Service (0x4c)
19	0.239335	Cisco_02:4e:13	Broadcast	RLDP	60	Network Loop Detection
20	0.258282	192.168.1.20	192.168.1.3	CIP	116	'stop_powerflex' - Service (0x4c)
21	0.258311	192.168.1.20	192.168.1.3	TCP	116	[TCP Retransmission] 44429 → 44818 [PSH, ACK] Seq=359 Ack=290 Win=1460 Len=62
22	0.260770	192.168.1.3	192.168.1.20	CIP	101	Success: 'stop_powerflex' - Service (0x4c)

Fig. 12 - Capture de trames réalisées depuis le PC Supervision avec l'émulateur de l'IHM

Nous avons réalisé la même opération, les mêmes effets provoquent les mêmes conséquences, nous pouvons visualiser l'ensemble des informations échangées entre l'automate et l'IHM (simulé avec l'émulateur de **Crimson**).

En conclusion de l'étude des échanges entre l'automate et l'IHM, le système n'est pas du tout sécurisé d'un point de vue cybersécurité, aucune protection n'est réalisée sur l'IHM (mot de passe faible, pas de filtrage IP, certificat non géré par une autorité de certification) et les données de commande de l'automate ne sont pas cryptées !

## Etude des échanges entre l'automate et le variateur PowerFlex

Nous allons maintenant nous intéresser aux échanges entre l'automate et le variateur **PowerFlex 1** en utilisant un convertisseur **Modbus RTU**. Vous trouverez l'ensemble des captures de trames réalisées dans le sous-dossier **Modbus RTU** du Drive Partagé :

### [Modbus RTU](#)

Nous décidons de lancer une capture de trames pendant le fonctionnement du moteur de la meule et nous allons l'analyser :

177	02/05/2024 14:49:13	IRP_MJ_READ	UP	STATUS_SUCCESS	01 03 21 00 00 07 0e 34	.....4	8	COM8
178	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_WAIT_ON_MASK)	DOWN					COM8
179	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_WAIT_ON_MASK)	UP	STATUS_SUCCESS	01 00 00 00	....	4	COM8
180	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_WAIT_MASK)	DOWN					COM8
181	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_WAIT_MASK)	UP	STATUS_SUCCESS	19 01 00 00	....	4	COM8
182	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_COMMSTATUS)	DOWN					COM8
183	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_COMMSTATUS)	UP	STATUS_SUCCESS	00 00 00 00 00 00 00 00 13 00 00 00 00 00 00 00 00 00	.....	20	COM8
184	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_COMMSTATUS)	DOWN					COM8
185	02/05/2024 14:49:13	IRP_MJ_DEVICE_CONTROL (IOCTL_SERIAL_GET_COMMSTATUS)	UP	STATUS_SUCCESS	00 00 00 00 00 00 00 00 13 00 00 00 00 00 00 00 00 00	.....	20	COM8
186	02/05/2024 14:49:13	IRP_MJ_READ	DOWN					COM8
187	02/05/2024 14:49:13	IRP_MJ_READ	UP	STATUS_SUCCESS	01 03 0e 06 1f 00 00 01 f4 00 7e 00 83 01 41 02 e2 af 95	.....ô.~.f.A.â•	19	COM8

Fig. 13 - Capture de trames réalisée sur le bus Modbus RTU

Regroupons toutes les trames qui ne correspondent qu'au **PowerFlex 1 (Adresse Modbus : 01)**. J'ai laissé volontairement la commande du **PowerFlex 2 (Adresse Modbus : 02)**, nous ne pourrions pas analyser de réponse car nous ne possédons pas le deuxième variateur. Nous pouvons attester que le système envoie des requêtes régulièrement sur le moteur de l'auget, ce qui donne le tableau suivant :

```
47 02/05/2024 14:49:09 IRP_MJ_READ UP STATUS_SUCCESS 02 03 40 01 00 01 c0 39
..@...À9 8 COM8

177 02/05/2024 14:49:13 IRP_MJ_READ UP STATUS_SUCCESS 01 03 21 00 00 07 0e 34
..!....4 8 COM8

187 02/05/2024 14:49:13 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 1f 00 00 01 f4
00 7e 00 83 01 41 02 e2 af 95 .....ô.~.f.A.â• 19 COM8
```

Fig. 14 - Capture de trames n°47, n°177 et n°187 réalisé sur le bus Modbus RTU

Intéressons-nous aux échanges **n°177** et **n°187** qui correspondent à une requête et une réponse entre l'automate et le variateur. Cependant, comme c'est la réponse qui nous intéresse, nous allons détailler la trame **n°187** :

```
187 02/05/2024 14:49:13 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 1f 00 00 01 f4
00 7e 00 83 01 41 02 e2 af 95 .....ô.~.f.A.â• 19 COM8
```

Enlevons tout le superflu pour ne laisser que les données utiles :

```
01 03 0e 06 1f 00 00 01 f4 00 7e 00 83 01 41 02 e2 af 95
```

Vous trouverez la documentation dans le Drive Partagé du Modbus, nous allons expliquer rapidement :

**01** : Adresse Modbus donc Powerflex 1

**03** : Lecture de Registres

**0e** : Longueur des Données donc 14 Octets, il reste 16 Octets car 2 octets sont réservés pour le CRC

**01 F4** : La documentation donne ce registre à lire pour la fréquence de fonctionnement du moteur en dixième d'Hertz :  $(01\ F4)_{16} \rightarrow (500)_{10} \rightarrow 50.0\ \text{Hz}$

**00 83** : La documentation donne ce registre à lire pour le courant de fonctionnement du moteur en centième d'Ampère :  $(00\ 83)_{16} \rightarrow (131)_{10} \rightarrow 1.31\ \text{A}$

Nous pouvons vérifier dans le programme **CCW** la configuration de la fréquence de la meule à 50 Hz (SpeedRef) :

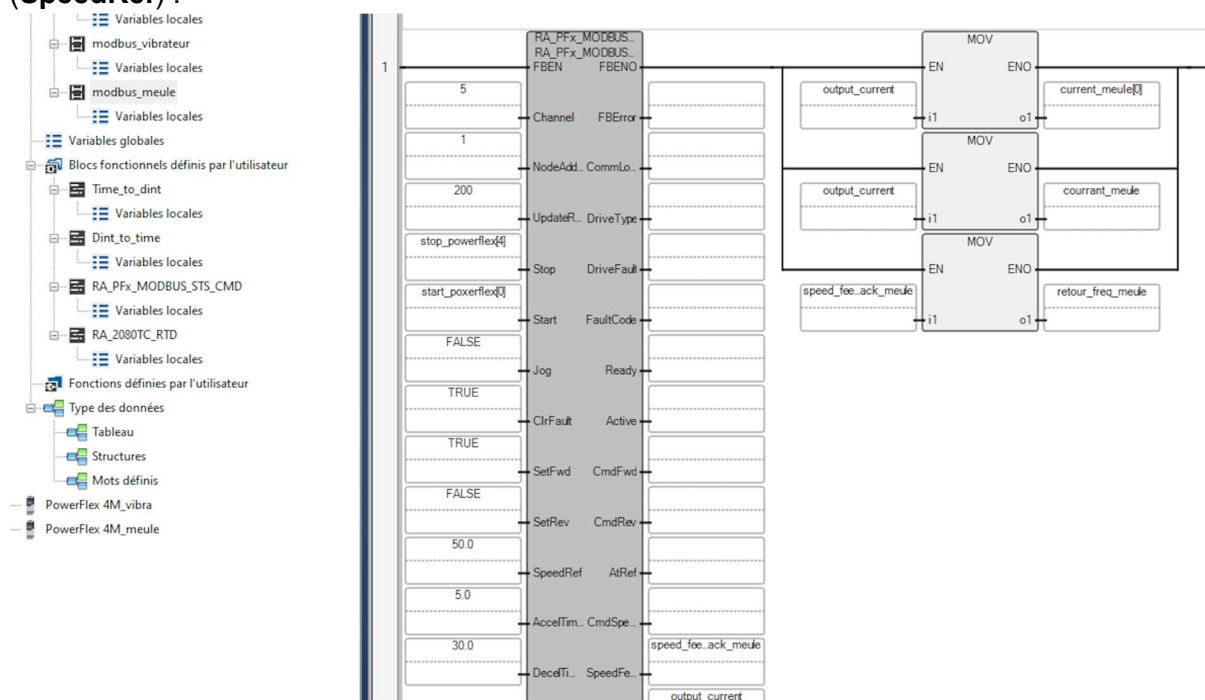


Fig. 15 - Configuration du moteur de la meule avec le protocole Modbus RTU

## Conclusion des études des échanges

Pour conclure ces 2 études, nous attestons :

- Que les échanges de communication entre l'automate et l'IHM ne sont pas chiffrés.
- Que les échanges de communication entre l'automate et les variateurs ne sont pas chiffrés.
- Que le système développé n'a pas été conçu dans un souci de prise en compte de risques liés à la cybersécurité.

Tant que le système reste autonome, mis à part la problématique liée à la sécurité du protocole **Modbus RTU**, cela n'est pas très gênant du moment que le système n'est pas relié au réseau de l'entreprise. Maintenant, l'entreprise réalise les limites d'un système autonome et elle souhaite pouvoir sécuriser son système au maximum !

## Piste d'amélioration envisagée et connexion du système à Internet

Nous allons nous intéresser à la connexion du système sur Internet mais nous n'avons pas répondu à la question : comment sécuriser le système ?

Concernant le protocole **Modbus RTU**, il n'y a malheureusement pas grand chose à faire, je vous conseille de lire cet excellent [article en anglais](#) qui rappelle que les protocoles **Modbus**, **Modbus RTU** et **Modbus TCP** ne peuvent pas être sécurisés. Il donne cependant des pistes de réflexions sur la sécurisation du **SI (Système d'Information)** et c'est ce que nous allons faire.

Concernant le protocole **CIP**, il existe un système [CIP Security](#) pour sécuriser les échanges entre l'automate et l'IHM. Malheureusement encore, ce protocole n'est pas disponible sur la gamme de produits **Micro 850** de chez **Allen-Bradley**, cette technologie n'est disponible que pour [les systèmes plus évolués de la gamme Rockwell Automation](#).

Il est donc impossible de sécuriser cette chaîne de production au niveau local. Cependant, comme nous souhaitons pouvoir accéder aux données du système sur Internet, nous allons sécuriser la connexion Internet avec l'ajout de 2 éléments importants :

- 1 **connexion VPN** devra être réalisée pour connecter le système au centre de données qui recueillera les informations et pour sécuriser les échanges de communication.
- 1 **pare-feu matériel** pour surveiller, bloquer et prévenir tout risque d'intrusion afin de mettre en place une stratégie de protection du système par rapport aux personnes malveillantes sur Internet.

Les aspects de cybersécurité ne doivent pas être négligés et ce pour 2 raisons :

- Il est nécessaire d'empêcher que les données soient divulguées sur Internet car très souvent, les systèmes qui ouvrent des brèches de sécurité sont les équipements qui paraissent inoffensifs (**IoT**, périphériques nomades, etc .....). Vous trouverez un excellent article ([payant](#)) sur **LeMonde.fr** qui explique que des hackers russes, pensant avoir piraté un barrage, se sont en fait attaqués à ... un moulin !
- Il faut surtout prendre en considération qu'il est possible de commander à distance le moulin en utilisant le protocole **CIP** et d'avoir une utilisation malveillante du système en faisant « sauter » les sécurités qui permettent de protéger le moulin. On peut « truquer » les consignes moteur (courant de consigne, fréquence de fonctionnement, etc ..... ) et désactiver les sécurités, le moteur peut se retrouver en dysfonctionnement pour de bon. Outre le fait que la chaîne de production est à l'arrêt, cela va engendrer des coûts supplémentaires pour réparer le système !

Toute cette partie, **VPN** et **pare-feu matériel**, sera détaillée dans la séquence pédagogique de ce dossier. Nous allons maintenant proposer une ingénierie logicielle afin de pouvoir surveiller les moulins à distance. C'est parti pour le Code !

## Analyse protocole Modbus RTU



```

47 02/05/2024 14:49:09 IRP_MJ_READ UP STATUS_SUCCESS 02 03 40 01 00 01 c0 39
..@...À9 8 COM8

117 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 04 00 1a
01 f4 4b be .. .....ôK¾ 13 COM8
127 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 4a 08 ..
...J. 8 COM8

137 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 04 00 18
01 f4 ea 7e .. .....ôê~ 13 COM8
147 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 4a 08 ..
...J. 8 COM8

157 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 03 21 00 00 07 0e 34
..!....4 8 COM8
167 02/05/2024 14:49:12 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 1f 00 00 01 f4
00 1d 00 3d 01 40 01 0a 85 f6 .....ô...=.@....ö 19 COM8

177 02/05/2024 14:49:13 IRP_MJ_READ UP STATUS_SUCCESS 01 03 21 00 00 07 0e 34
..!....4 8 COM8
187 02/05/2024 14:49:13 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 1f 00 00 01 f4
00 7e 00 83 01 41 02 e2 af 95 .....ô~.f.A.â• 19 COM8

197 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 04 00 19
01 f4 bb be .. .....ô»¾ 13 COM8
207 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 4a 08 ..
...J. 8 COM8

217 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 04 00 18
01 f4 ea 7e .. .....ôê~ 13 COM8
227 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 10 20 00 00 02 4a 08 ..
...J. 8 COM8

237 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 03 21 00 00 07 0e 34
..!....4 8 COM8
247 02/05/2024 14:49:14 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 2f 00 00 01 f4
00 ba 00 76 01 41 03 ed a6 28 ...../...ô.°.v.Ä.î| ( 19 COM8

257 02/05/2024 14:49:15 IRP_MJ_READ UP STATUS_SUCCESS 01 03 21 00 00 07 0e 34
..!....4 8 COM8
267 02/05/2024 14:49:15 IRP_MJ_READ UP STATUS_SUCCESS 01 03 0e 06 2f 00 00 01 f4
00 a9 00 78 01 41 03 9d ec cc ...../...ô.©.x.Ä. îï 19 COM8

Adresse PowerFlex 1 : 01 : Variateur Moteur Meule
Adresse PowerFlex 2 : 02 : Variateur Moteur Vibreur Auger

Lecture : 03
Ecriture Multiple : 10 (ou 16 en Décimal)

2100 : Adresse Début 8448 en Décimal en Lecture
2000 : Adresse Début 8192 en Décimal en Ecriture

01 F4 : 500 : Correspond à 50 Hz

```

0e : 14 Octets de Longueur  
CRC : 2 Octets

00 83 : 131 : 1.31 A  
00 76 : 118 : 1.18 A  
00 78 : 120 : 1.20 A