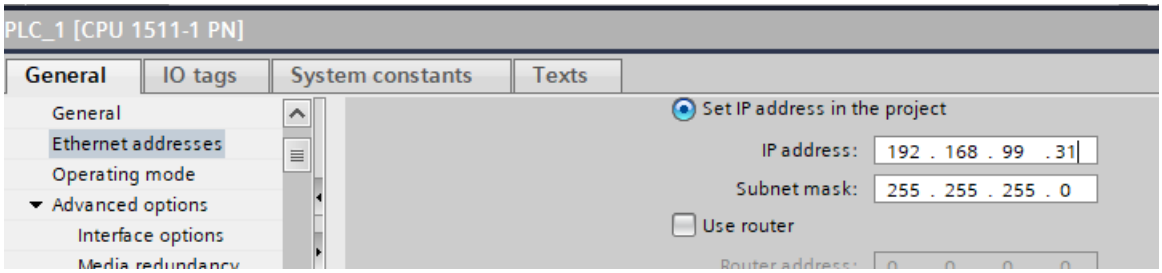
1 Introduction : manipulation S7300

Q1. Suite à la manipulation faite par le professeur sur un S7-300, expliquer quel est le risque d'utiliser une communication en clair entre l'automate et le poste d'ingenierie qui sert à le programmer.

2 Manipulation S71500

- 🛠 Créer un projet nommé ***SAé13_S71500***, passer en vue de projet. Dans les propriétés du projet, à l'onglet « protection », autoriser la simulation.
- 🛠 Créer dans le projet un nouvel automate de type S71511-1PN. Choisi la référence 6ES7 511-1AK02-0AB0. On doit normalement vous proposer de suivre un « PLC Security Wizzard »
- 🛠 Lui attribuer une adresse Ethernet



2.1 PLC Security

2.1.1 Protection of the configuration PLC Data.

On vous propose dans un premier temps de choisir un mot de passe pour la configuration de l'automate.

Q2. Que protège ce mot de passe ?

- 🛠 Configurer un mot de passe de configuration de l'automate, puis cliquer sur « Next »

2.1.2 Mode for PG/PC and HMI Configuration

Le PG/PC (Programmier Geräte / Personal Computer) est le poste d'ingénierie,
Le HMI (Human Machine Interface) est le panneau tactile permettant à l'opérateur de piloter la production.

Q3. Quels sont les deux modes qui sont proposés entre l'automate d'une part et le PG/PC ou HMI d'autre part ? Qu'est-ce qui change entre ces deux modes ? Quel est l'intérêt de choisir un mode plutôt que l'autre en fonction de critères de sécurité ?

- 🛠 Configurer une communication sans chiffrement, puis cliquer sur « Next »

2.1.3 PLC access protection.

On vous propose de choisir un mot de passe pour l'accès à l'automate.

Q4. Que protège ce mot de passe ?

- 🛠 Configurer un mot de passe d'accès à l'automate (différent de celui de configuration), puis cliquer sur « Next ». Une fenêtre « overview » permet de visualiser la configuration de sécurité qui a été effectuée. Vérifier que tout est conforme à la configuration effectuée, puis cliquer sur « Finish »

2.2 Simulation de l'automate

On désire que l'alarme fonctionne avec un voyant clignotant.

2.3 Tests

Q5. Charger la configuration de l'automate. Quel mot de passe vous demande-t-on ?

Q6. Modifier le mot de passe de configuration, parvenez-vous à charger un programme dans l'automate ?

1. Renforcement du mot de passe

Aller dans les configurations de sécurité dans l'arborescence.

Q7. Où peut-on modifier la force des mots de passe que l'utilisateur doit saisir pour accéder aux données de l'automate ?

🛠 Augmenter la robustesse du mot de passe de l'utilisateur.

2.4 Embedded Webserver

On désire accéder à l'automate via son interface Web.

🛠 Dans la configuration, activer le webserver de l'automate. Configurer le serveur Web de l'automate pour pouvoir changer le mode de l'automate et pour permettre la lecture et l'écriture de variables. Définir un utilisateur et un mot de passe. Choisir un échange sans chiffrement des données.

🛠 Transférer la nouvelle configuration.

🛠 Ouvrir un navigateur sur la machine physique et rentrer l'adresse de l'automate dans la barre d'adresse. Se logguer et vérifier qu'il est possible de changer le mode de fonctionnement (RUN ou STOP) de l'automate.

Q8. Quel risque est associé selon vous à l'utilisation d'une telle interface ?

Q9. Ouvrir le logiciel Wireshark dans la machine physique et lancer la capture sur l'interface utilisée pour communiquer entre la machine physique et la machine virtuelle. Lancer le navigateur dans la machine physique et se connecter au serveur Web de l'automate. Se logguer. Qu'observe-t-on dans la capture de trame ?

Q10. Reproduire l'expérience de la question précédente, mais en ayant activé la connexion avec chiffrement des données. Quelle différence observe-t-on dans la capture de trame ?

3 Synthèse

Mot de passe	Protège l'accès à :	Utilisateurs concernés
Configuration		
Accès Automate		
Web		

Mesures supplémentaires prises pour protéger l'automate des cyberattaques ?