Content Type	Alert
Article #	000032848
Title	SIDirect and Edge/SITIA connection to secured Siemens SIMATIC S7-1200/S7-1500 PLCs
Legacy DocId	
Confidence	Expert Reviewed
Published On	2/7/2022

Known issues connecting to password-secured Siemens S7-1200/S7-1500 PLCs

UPDATE NOTES

- **February 6, 2022**: Original document published
- **April 29, 2024**: Updated for **OI SIDirect 2023 R2**, **Edge 2023(SITIA driver v1.10.0.0)**, and **Siemens TIA Portal v19**

BACKGROUND

You can secure an S7-1200 or S7-1500 PLC in the TIA Portal STEP 7 project's **Protection & Security** configuration using the **Access Level** setting (Figure 1 below).

The **Access Level** radio button is the default level that is utilized when there is no other password match found at a less restrictive level, or when no password is utilized by the connecting client. Secured customer PLCs are typically set to **No Access** and passwords are defined at all the less-restrictive access levels to ensure that PLC access is not possible without a valid password from a client, such as the **AVEVA SIDirect Communication Driver**.

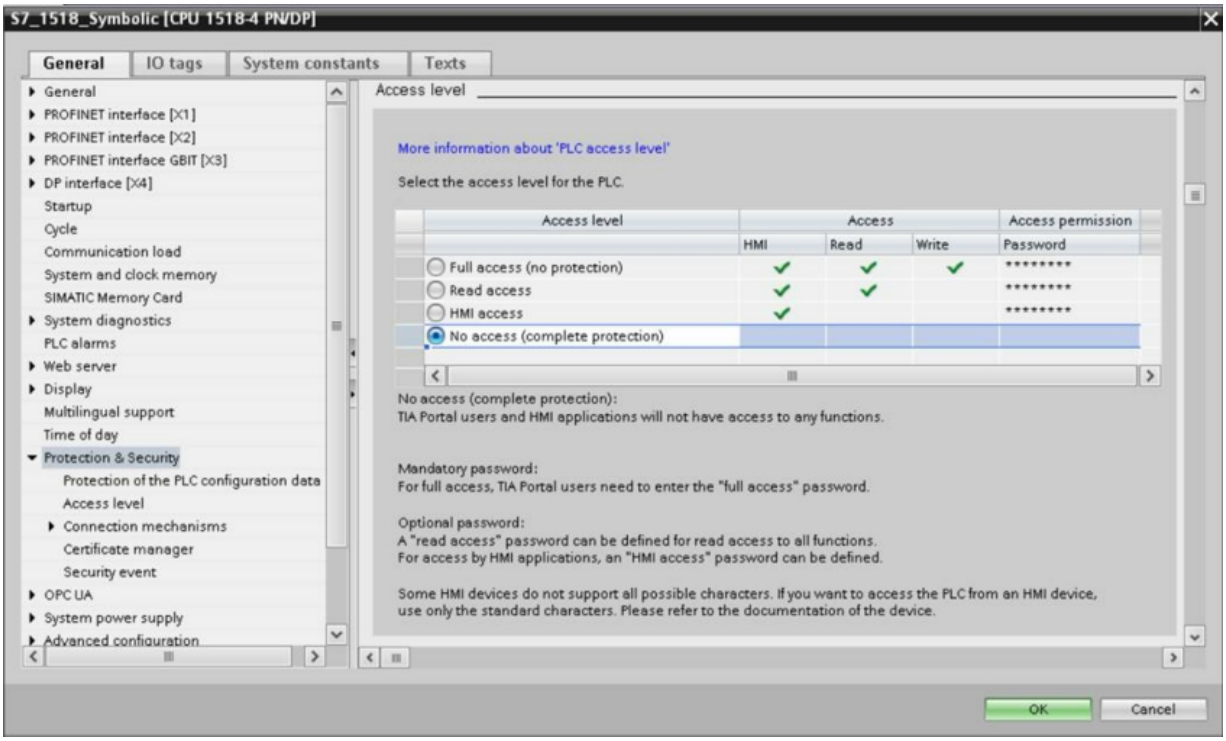

Figure 1: PLC Access Level security settings

In the TIA Portal configuration, you enforce certificate-based security by enabling **Only allow secure PG/PC and HMI communication** (Figure 2 below).

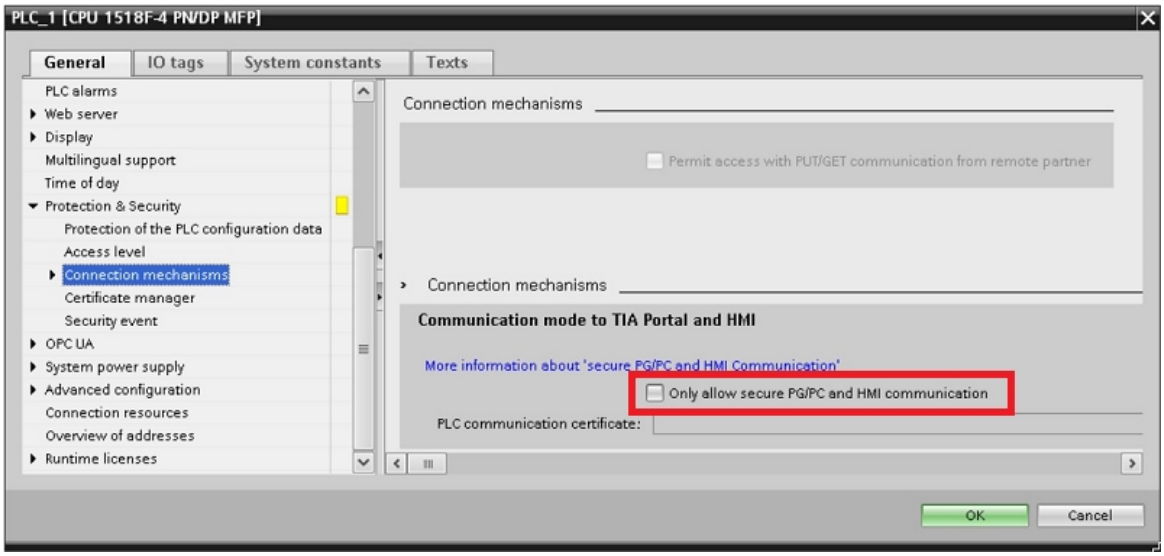

Figure 2: Certificate-based security configuration

From TIA Portal v19 release with S7-1500 on firmware v3.1.x or later, Security Wizard introduces an additional step for **Access Control** configuration. Traditional Access Control to the PLC can still be established via the **Legacy Access Control Levels** (No Access Failsafe/No Access/Read Access/HMI Access/Full Access) with their respective local passwords. Otherwise, Access Control is achieved through the project user assigned with roles associated with the runtime rights for the respective Access Control levels in '**Users and Roles**' under Protection & Security section.

Note: All of the following issues must be addressed with their associated solutions applied.

ISSUE #1

Software affected: AVEVA SIDirect Communication Driver versions 2020 R2 SP1 and 2020 R3. This issue is not present in older SIDirect releases and the issue occurs regardless of the PLC firmware version.

Issue: Attempting to configure a symbolic connection to a password-secured S7-1200/S7-1500 PLC using a valid password always results in a **Connection Failed!** message and communication cannot be established (Figure 3 below).

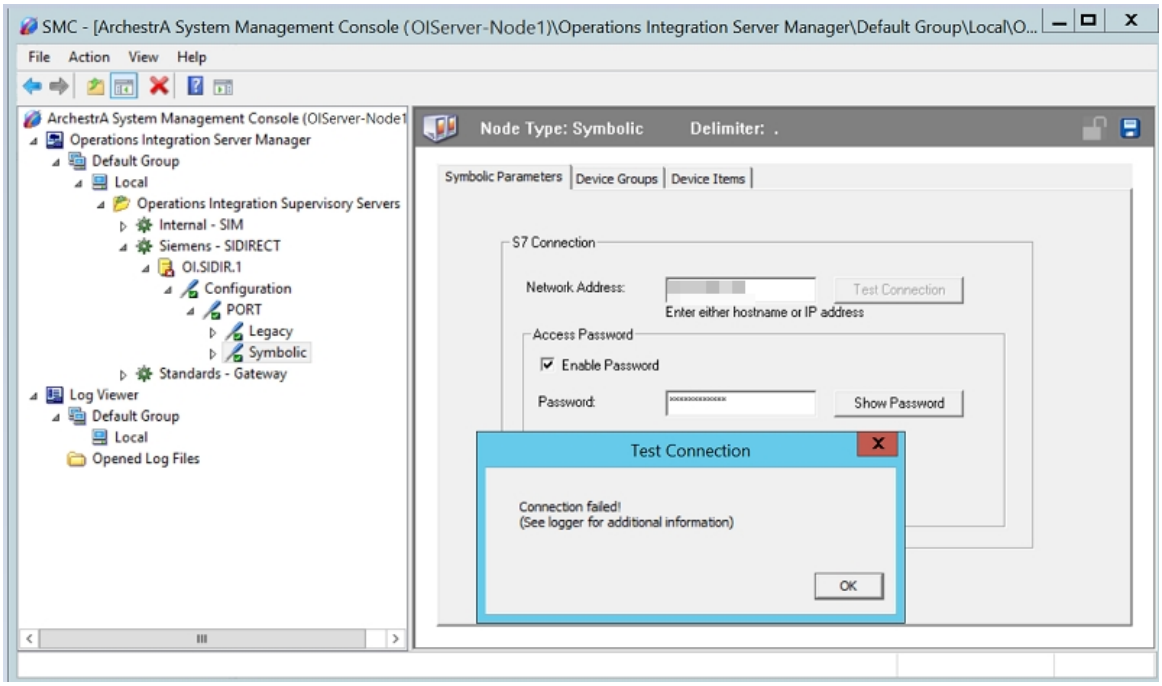

Figure 3: Failed connection test

The following messages will appear in the SMC log:

Warning	CONFIG_SI_S7PlusPLC	Connect to <*PLC IP Address*> failed !
Warning	CONFIG_SI_S7PlusPLC	... check if PLC Network Address is configured correctly.
Warning	CONFIG_SI_S7PlusPLC	... check if S7-1200 PLC is running firmware V4.0 or newer.

Warning CONFIG_SI_S7PlusPLC ... check if S7-1500 PLC is running firmware V1.5 or newer.

ISSUE #1 SOLUTION

Hotfix IMS-1682485 is available to correct this issue. Please contact your technical support representative to obtain the fix. Be sure to specify which version of SIDirect is being utilized so the correct version of the fix can be delivered. This Hotfix has been merged to CDP 2023 release and later versions, so upgrading is an alternate solution.

ISSUE #2

Software affected:

- **AVEVA SIDirect Communication Driver - all versions** (2023 R2 is the current release at the time of this document's publish date)**.**
- **AVEVA Edge SITIA Driver - all versions** (Edge 2023 / SITIA v1.10.0.0 is the current release at the time of this document's publish date).

Relevant PLC information: Traditionally **PLC Access Level** security is set to **No Access** (complete protection), and passwords are defined for all less restrictive **Access Levels**. Starting with **S7-1500 firmware v3.1.x in TIA Portal v19**, Access Control to the PLC can be enabled or disabled. If it is enabled, there is a checkbox option for using the **Legacy Access Control** via **Access Levels**. If this option is not chosen, **Access Control** will be authenticated with the activated project user created in '**Users and Roles**' under **Security Settings** section of the project who has been assigned with the role associated with the respective runtime rights for these **Access Levels**.

Issue: Prior to S7-1200 firmware v4.5.x and S7-1500 firmware v2.9.x, even if the **Access Level** was set to **No Access**, SIDirect/SITIA could connect to a PLC if a valid password was entered in the configuration that matched any one of the less restrictive levels of access. The matched level would be enforced by the PLC for driver communications.

When S7-1200/S7-1500 firmware is upgraded to v4.5.x/v3.0.x respectively, if the PLC **Access Level** is set to **No Access**, SIDirect/SITIA cannot connect nor read data, even with a valid password. The same failure of connection happens for S7-1500 firmware v3.1.x or later if **Access Control** is enabled.

ISSUE #2 SOLUTION

Option #1: Rollback the PLC firmware version prior to S7-1200 firmware v4.5.x and S7-1500 firmware v2.9.x.

Option #2: In case of S7-1200 firmware v4.5.x or S7-1500 firmware v2.9.x/v3.0.x, the PLC **Access Level** security needs to be set to a choice other than **No Access**, then SIDirect/SITIA can connect to the PLC without using any password. The PLC will allow reads and writes, regardless of the selected **Access Level**, similar to the **Full Access** setting (Figure 4 below).

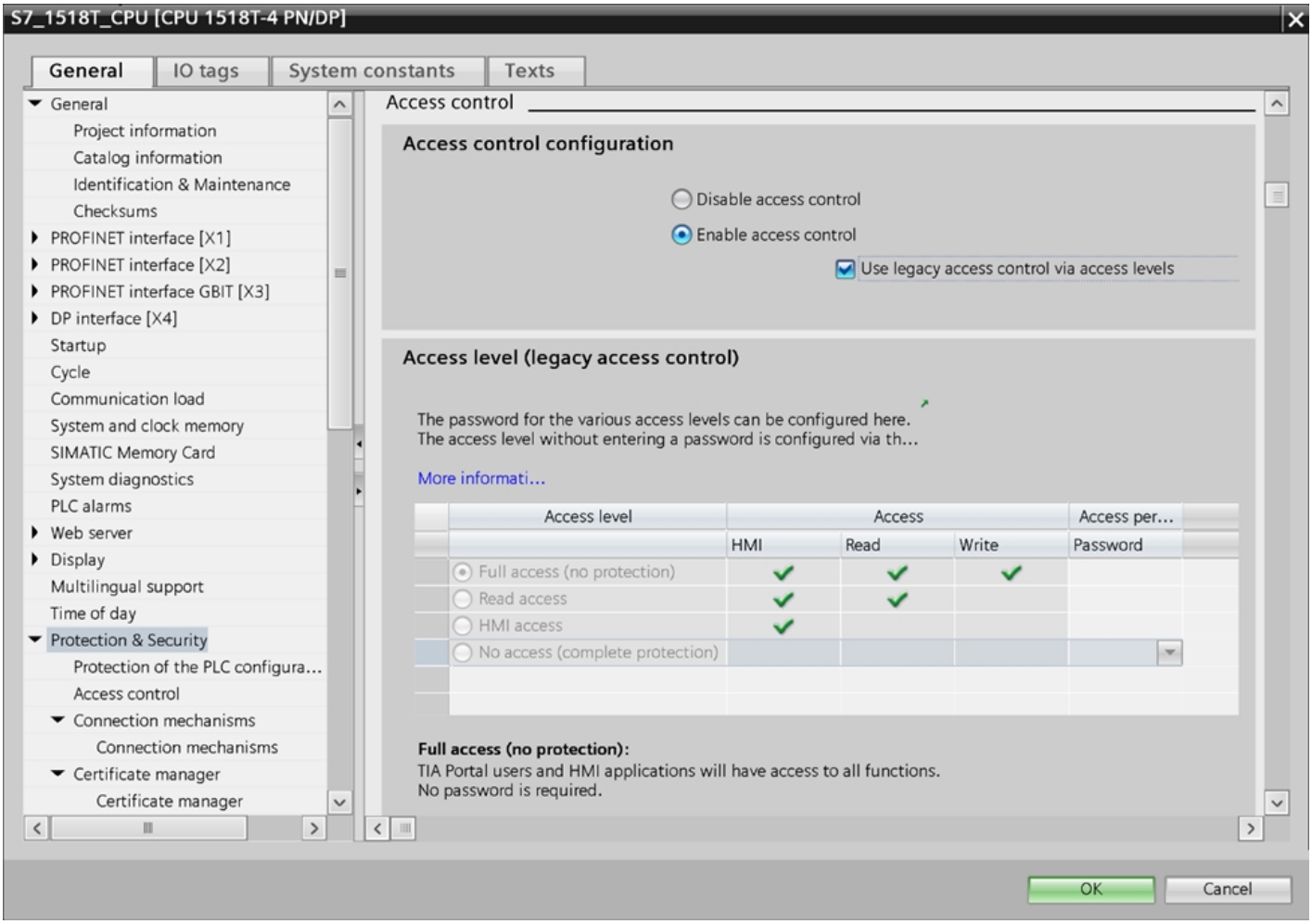

Figure 4: Legacy Access Control Configuration

In case of S7-1500 firmware v3.1.x or later, with **Access Control** disabled, it allows SIDirect/SITIA connection without security. If **Access Control** is enabled, create an Anonymous User with the respective runtime rights for the desirable Access Levels (Full Access/Read Access/HMI Access) in '**Users and Roles**' under Security Settings section of the project (Figures 5 and 6 below). After activating the Anonymous User, The Full Access is then displayed as selected in the Access Level column as shown in Figure 4.

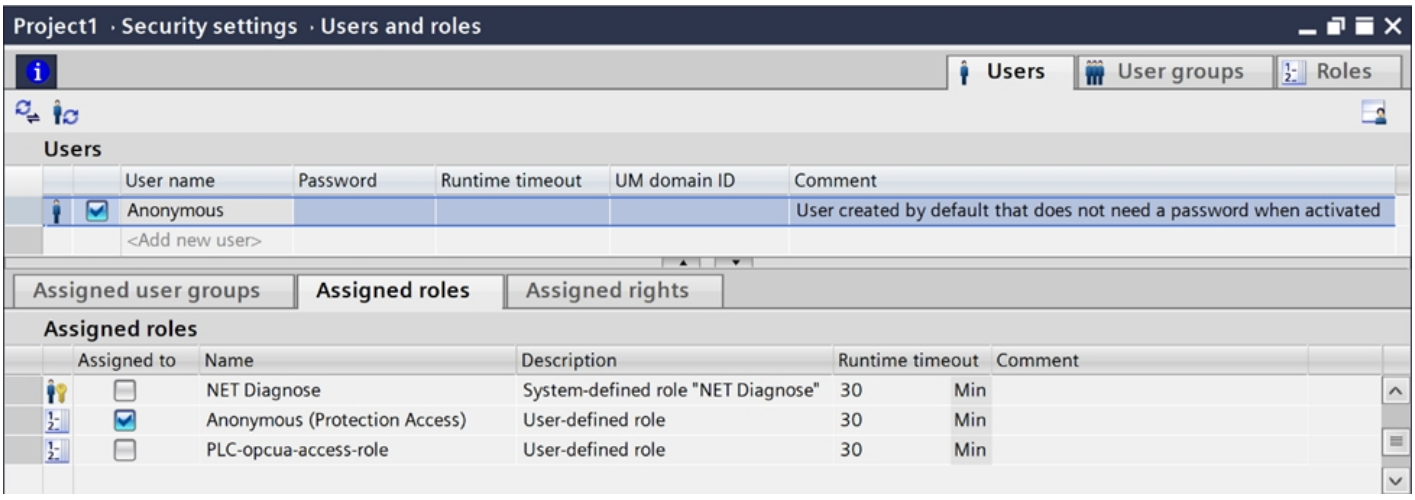

Figure 5: Users and Roles Configuration for Security Settings

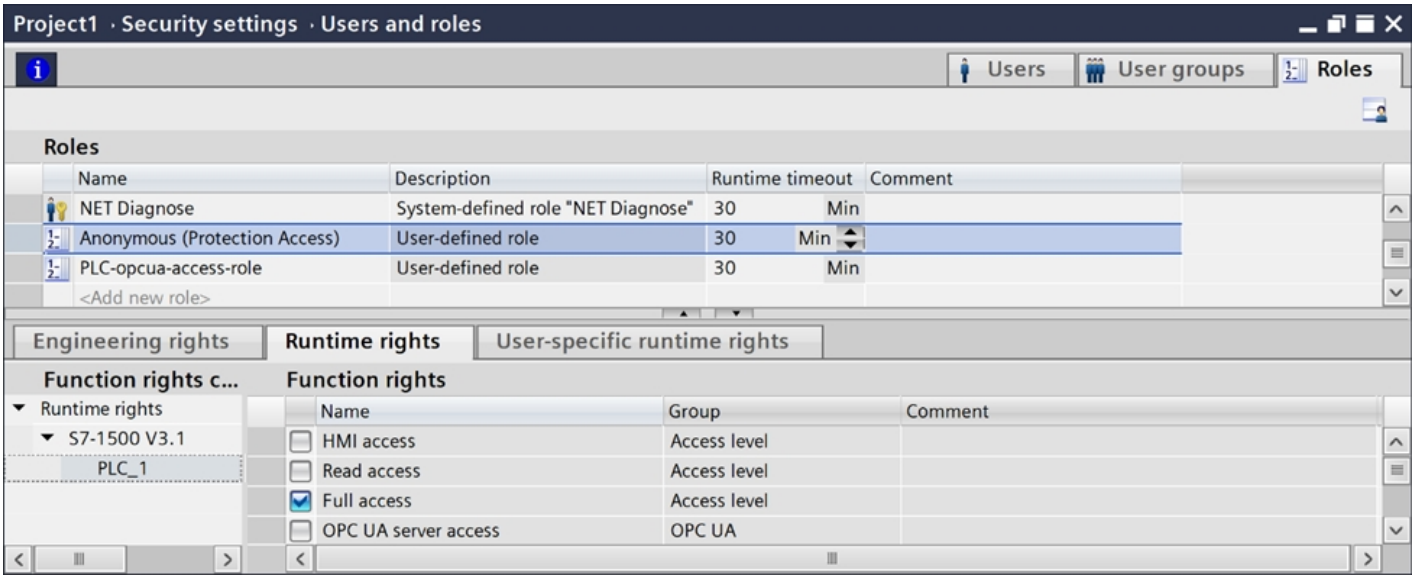

Figure 6: User role assigned with specific Access Level runtime rights

IMPORTANT NOTE! The PLC appears to require a password, but does not validate the password.

It is possible that this workaround creates an unsecure condition where any client can connect with **Full Access** as long as they use any valid or invalid password. Therefore this workaround may not be advisable in all situations and a risk assessment should be conducted.

Note: This article will be updated with any new information that is discovered.

ISSUE #3

Software affected:

- **AVEVA SIDirect Communication Driver - all versions** (2023 R2 is the current release at the time of this document's publish date)**.**
- **AVEVA Edge SITIA Driver - all versions** (Edge 2023 / SITIA v1.10.0.0 is the current release at the time of this document's publish date).

Relevant PLC information: For **S7-1200/S7-1500 with TIA Portal v17** and later, **Only allow secure PG/PC and HMI communication** is enabled by default (certificate-based security).

Note: Impacts symbolic communication method.

Issue: As of version 2023 R2, SIDirect does not support certificate-based secured communication to Siemens PLCs, therefore communications cannot be established if **Only allow secure PG/PC and HMI communication** is enabled. This is also not supported by SITIA as of version 1.10.0.0.

ISSUE #3 SOLUTION

Workaround: Disable the **Only allow secure PG/PC and HMI communication** configuration option checkbox in the TIA Portal configuration (Figure 7 below). Disabling the **Only allow secure**...option disables certificate-based security.

AVEVA Technical Support strongly recommends conducting a risk assessment before disabling this setting.

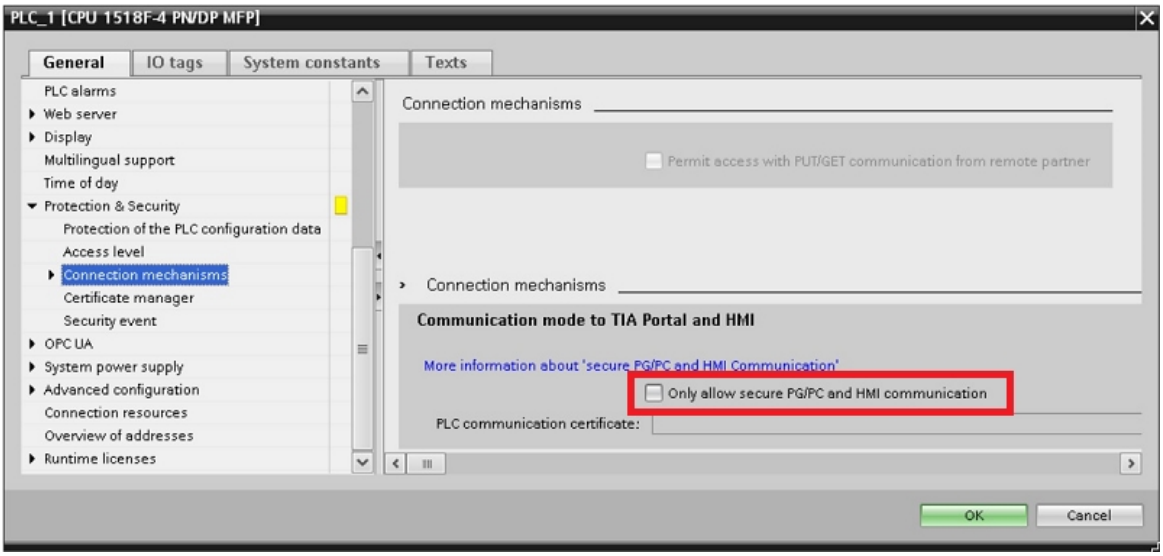

Figure 7: Secure communication configuration