

SIEMENS



Industry Online Support

Home

TIA Portal Project Upgrader

TIA Portal

<https://support.industry.siemens.com/cs/ww/en/view/109811744>

Siemens
Industry
Online
Support



Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. **The application examples are not subject to standard tests and quality inspections of a chargeable product and may contain functional and performance defects or other faults and security vulnerabilities. You are responsible for the proper and safe operation of the products in accordance with all applicable regulations, including checking and customizing the application example for your system, and ensuring that only trained personnel use it in a way that prevents property damage or injury to persons. You are solely responsible for any productive use.**

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. Any further use of the application examples is explicitly not permitted and further rights are not granted. You are not allowed to use application examples in any other way, including, without limitation, for any direct or indirect training or enhancements of AI models.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice and to terminate your use of the application examples at any time. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://www.siemens.com/global/en/general/terms-of-use>) shall also apply.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit

<https://www.siemens.com/cybersecurity-industry>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://www.siemens.com/cert>.

Table of contents

Legal information	2
1 Introduction	4
1.1 Overview	4
1.2 Version Compatibility and Selection	4
1.3 Components used	4
2 Engineering	6
2.1 Software setup	6
2.2 Managing user rights	6
3 Software Operation	8
3.1 Overview	8
3.2 Operation UI	8
3.3 Operation CLI	13
3.4 Operation python	14
3.5 Error handling	14
3.6 Known problems	14
4 Appendix	15
4.1 Service and support.....	15
4.2 Links and literature	16
4.3 Change documentation	16

1 Introduction

1.1 Overview

This application upgrades TIA Portal projects to the current version using TIA Portal Openness (e.g. from V15 to V17).

The solution offers the following advantages:

- Automatic upgrade the version of your TIA Portal project
- Batch update of the project can be carried out
- Automatic compile the project after project upgraded
- An update log shows the status

1.2 Version Compatibility and Selection

- **Minimum Requirements for Upgrade:** Projects from version V13 SP1 and onwards can be successfully upgraded. However, projects below this version cannot undergo the upgrade process.
- **Selection of Target Version:** The application allows users to choose the target version based on the installed versions of TIA Portal. For instance, if only TIA Portal V19 is installed, then only this version is available as a target option.
- **Support for Multiple Installed TIA Portal Versions:** In case multiple TIA Portal versions are installed on the system, they are automatically displayed in the target version dropdown menu. Users can select the desired target version based on their installed software.
- **Automatic Detection of Future Versions:** Future TIA Portal versions are automatically recognized by the upgrader and can be selected as target versions. This ensures that the application remains compatible with the latest versions, including TIA Portal V20 and beyond.

1.3 Components used

This application example has been created with the following hardware and software components:

Table 1-1

Component	Number	Article number	Note
STEP 7 Professional V17	1	6ES7822-1AA06-0YA5	-
TIA Portal Openness	1	-	-
Microsoft Visual Studio 2019	1	-	-

This application example consists of the following components:

Table 1-2

Component	File name	Note
UI Executable	Siemens.TiaPortalProjectUpgraderUi.exe	Application for the UI usage
CLI Executable	Siemens.TiaPortalProjectUpgraderCli.exe	Application for the CLI usage
Python script	upgrader.py	Raw python version of the TIA Portal Project Upgrader for usage directly with python
Third-Party Software Information	Multilingual_ReadMe_OSS.html	Third-Party Software Information
Manual	109811744_TIAPortalProjectUpgrader_DOC_V2_0_5_en.pdf	This document

2 Engineering

2.1 Software setup

Install TIA Portal V17 or higher version.

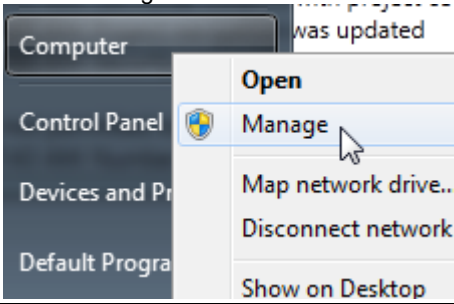
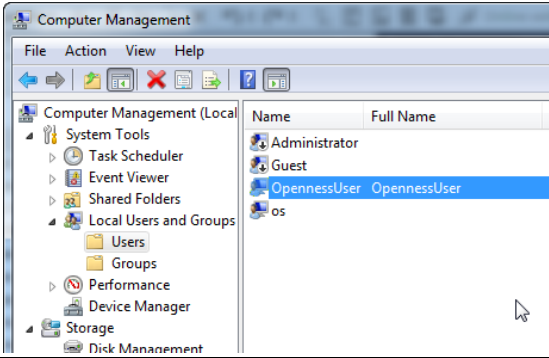
Note

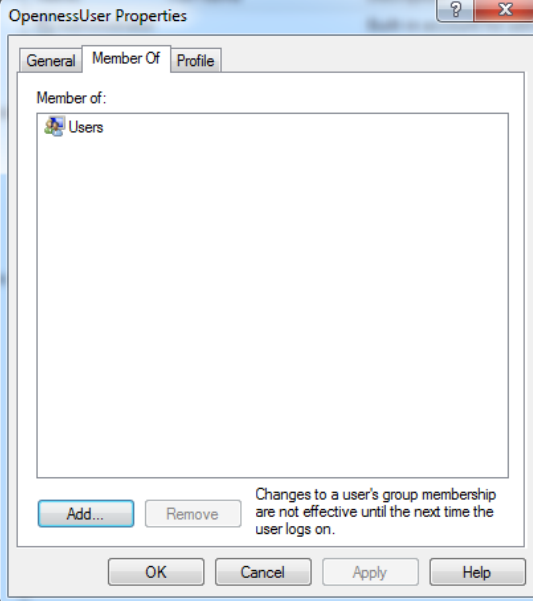
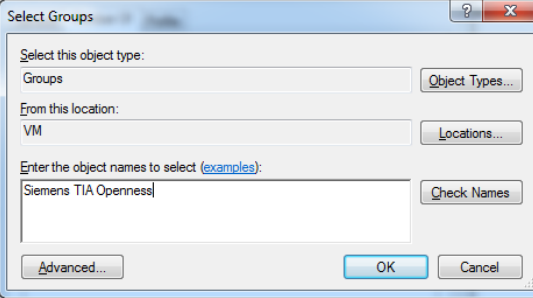
TIA Portal Openness is included in the delivery of STEP 7 V17 or WinCC V17 and is installed by default.

2.2 Managing user rights

In order to use or create a TIA Portal Openness application, the user has to be added to the "Siemens TIA Openness" user group.

Table 2-1

No.	Action
1.	Right click "Computer" in the windows taskbar and select "Manage". 
2.	Open "Local Users and Groups and Groups > Users" and double click the user. 
3.	Go to the "Member Of" tab and click the "Add" button.

No.	Action
	
4.	<p>Enter "Siemens TIA Openness" and confirm by pressing OK.</p> 
5.	Close the opened dialog boxes and log in again.

3 Software Operation

3.1 Overview

Three types of execution are available.

First one is the UI.

The second one is the usage of the CLI.

The CLI “Siemens.TiaPortalProjectUpgraderCli.exe” provides some CLI arguments where the user is able to configure the upgrade process. The file “Siemens.TiaPortalProjectUpgraderCli.exe” is the generated executable version of the upgrader.py Python script. The “Siemens.TiaPortalProjectUpgraderCli.exe” file is necessary for the usage of the UI.

The last type of execution is to modify and run the upgrader.py Python script manually, also over the CLI or directly with adapted arguments.

3.2 Operation UI

Run the TiaPortalProjectUpgraderUI.exe

Figure 3-1

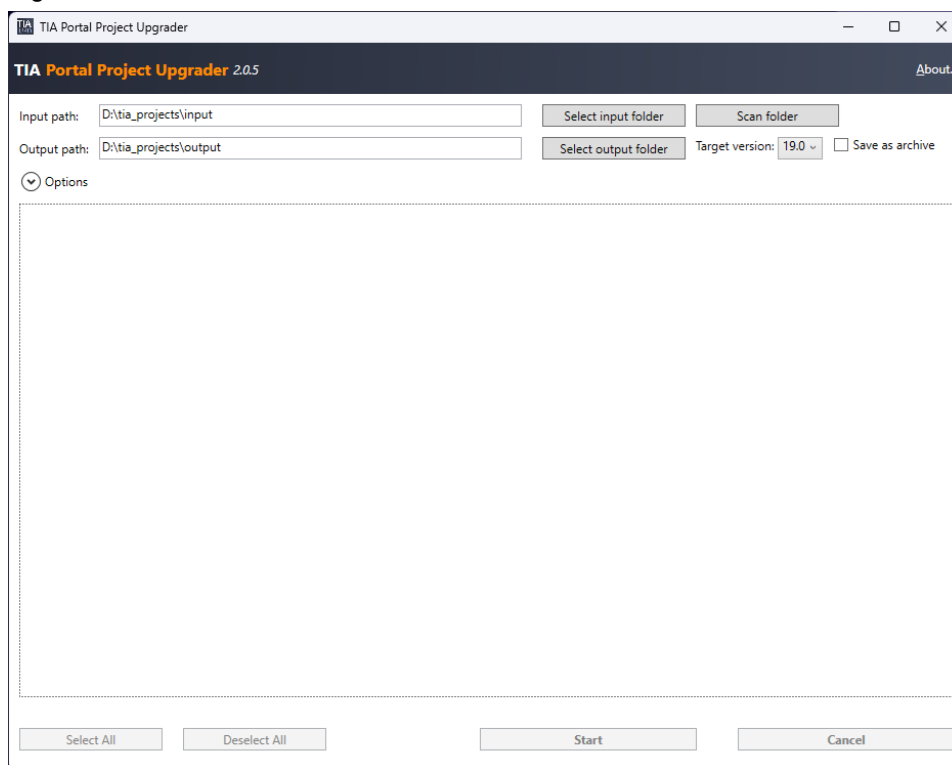
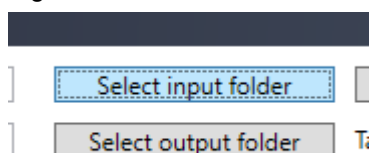
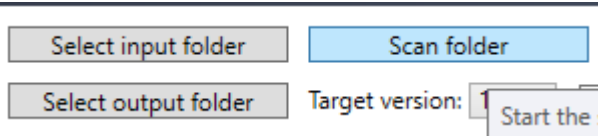


Figure 3-2



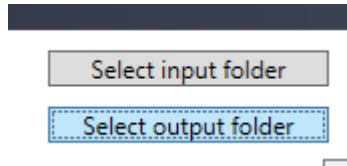
Click “Select input folder” and choose the folder where the TIA Portal projects to be upgraded are stored. After selecting the directory, the scan of the folder will be automatically started.

Figure 3-3



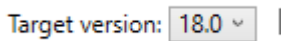
Click “Scan folder” to start the scan of the selected directory.

Figure 3-4



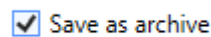
Click “Select output folder” to choose the folder where to store the upgraded projects.

Figure 3-5



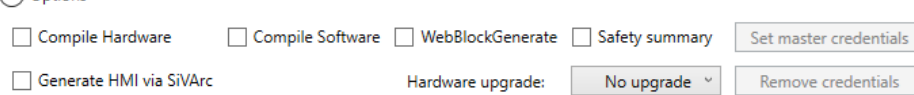
The combo box “Target version” shows available target versions of the installed TIA Portal version.

Figure 3-6



The checkbox “Save as archive” means that the project is saved as an archived file after upgrading.

Figure 3-7



Under the “Options,” it is possible to set parameters for the upgrading process.

“Compile Hardware”: click the checkbox to compile the hardware in the project.

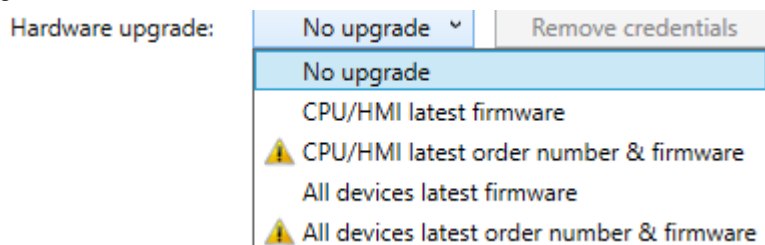
“Compile Software”: click the checkbox to compile the software in the project.

“Generate HMI via SiVArc”: click the checkbox to trigger SiVArc generation if used in the project already (License required).

“WebBlockGenerate”: click the checkbox to generate Web-DBs in the PLC if used in the project already.

“Safety summary”: creates a safety printout for the PLC's and points it to the file, (UserFiles) of the output project.

Figure 3-8

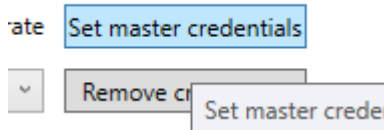


The “Hardware Upgrade” combo box shows available options for upgrading the hardware in the project.

Menu	CPU1511F 6ES7 511-1FK00-0AB0 V1.7	ET200SP DI 8x24VDCST 6ES7 131-6BF00-0BA0 V1.0
CPU/HMI latest firmware	6ES7 511-1FK00-0AB0 V1.8	6ES7 131-6BF00-0BA0 V1.0
CPU/HMI latest Order Number/firmware	6ES7 511-1FL03-0AB0 V3.0	6ES7 131-6BF00-0BA0 V1.0
All devices latest firmware	6ES7 511-1FK00-0AB0 V1.8	6ES7 131-6BF00-0BA0 V1.1
All devices latest Order Number/firmware	6ES7 511-1FL03-0AB0 V3.0	6ES7 131-6BF01-0BA0 V0.0

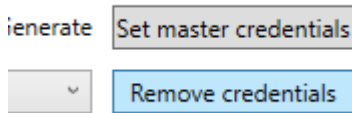
All devices = ET200MP modules, ET200SP modules, etc.

Figure 3-9



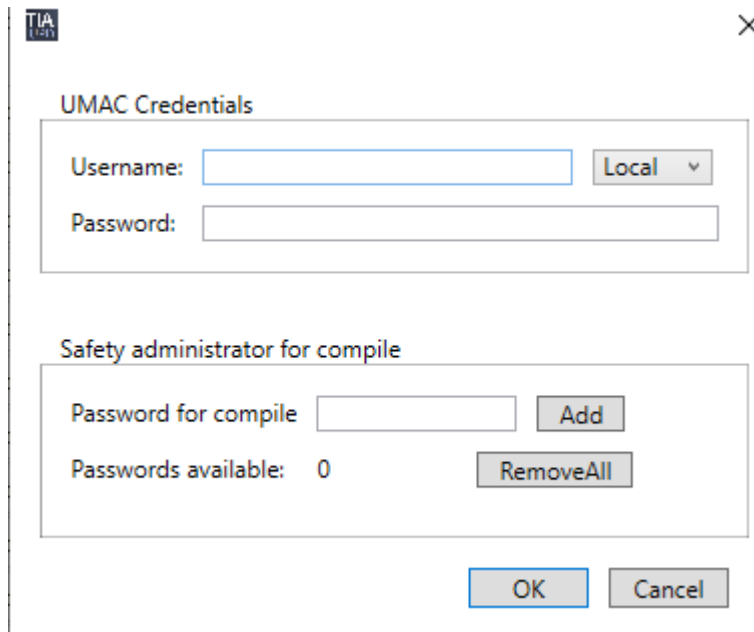
“Set master credentials” shows a dialog where the user is able to set UMAC Credentials for all listed projects. Credentials will be used if some of the projects are protected.

Figure 3-10



“Remove credentials” just removes set master credentials.

Figure 3-11



If the “Set master credentials” button is clicked, a dialog is shown in the message window to provide the possibility to set UMAC Credentials and Safety administrator passwords for compiling.

Figure 3-12

In the “UMAC Credentials” part, there is the possibility to set credentials for protected projects. These credentials will be used to open the project. It is possible to switch the user type between “Local” and “Global” user.

Note

Master Credentials will be set for all projects and will be used ONLY if the project is protected. So, if some projects are not protected, it does not matter if credentials are set or not.

Figure 3-13

In the “Safety administrator for compile” part, the user is able to add passwords to a list. These passwords will be used for any “knowhow” protected device if compile is required.

Note

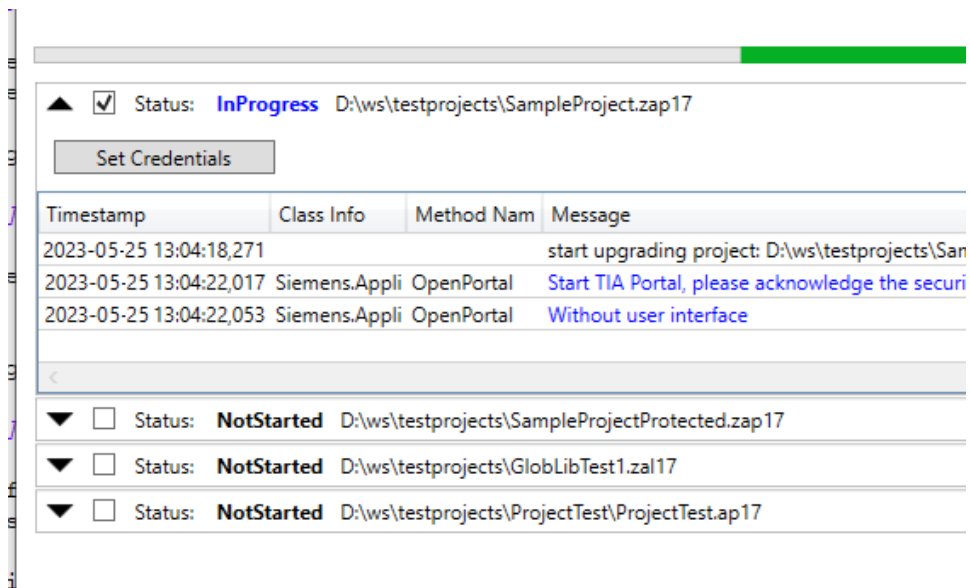
The list of passwords will be used only if a knowhow protected device is detected. In this case, each password will be tried to set for the device until one of the provided passwords matches.

Figure 3-14

<input type="checkbox"/>	Status: NotStarted	ProjectUpgrader_TestWeb_HMLzap17
<input type="checkbox"/>	Status: NotStarted	Project_PW_missingWinCC.zap17
<input type="checkbox"/>	Status: NotStarted	ProtectedProject.zap17
<input checked="" type="checkbox"/>	Status: NotStarted	StyleGuide_DemoProject.zap15
<input checked="" type="checkbox"/>	Status: NotStarted	GlobLibTest1.zal17
<input type="checkbox"/>	Status: NotStarted	DigiMachine_V18_LSafe.ap18

Listed projects after scanning the input folder. With the button “Start,” the user is able to start upgrading all selected projects.

Figure 3-15



Each project is expandable. When an entry is expanded, the log of the upgrading process is visible. With the button “Set Credentials,” the user is able to set their own credentials for the selected project.

Note

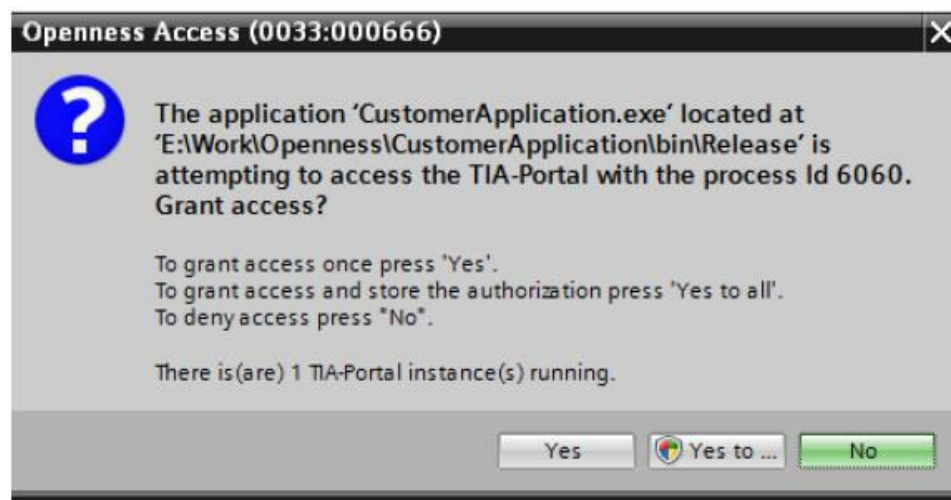
In this case, if master credentials are already set, the selected project's credentials will be overwritten.

If the checkbox is set, the user is able to start the upgrading process only for the selected projects.

After clicking the “Start” button, a message is shown in the message window to remind you to confirm the security information dialog.

When starting your application for the first time, the following security message will appear:

Figure 3-16



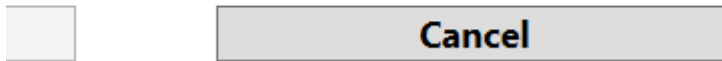
Confirm the message with “Yes” in order to permit access once.

Confirm the message with “Yes to all” in order to always permit access to this application.

Click “No” to deny access – the application cannot continue in this case.

After confirming the security message, the application will start to upgrade, and the message window will have the information.

Figure 3-17



“Cancel Upgrade“ will cancel the upgrade of the project.

3.3 Operation CLI

“Siemens.TiaPortalProjectUpgraderCli.exe” can be executed directly over the CLI usage:

```
usage: Siemens.TiaPortalProjectUpgraderCli.exe
       [-h] [--archive]
       [--software] [--hardware]
       [--sivarc] [--webblock]
       inputpath outputpath version
       {nouppgrade, cpuhmifirmwareonly,
       cpuhmifull, alldevicesfirmwareonly,
       alldevicesfull}
```

example:

```
Siemens.TiaPortalProjectUpgraderCli D:\ws\test_tiascripting\input\Test\Test.ap16
D:\ws\test_tiascripting\output 18.0 cpuhmifirmwareonly --hardware --software
```

The upgrade process was started with V18 as target version and optional hardware and software compile, also the upgrader of the hardware was set to upgrade all CPU's and HMI's to the latest firmware.

Positional arguments	Description
inputpath	set input path of the project file
outputpath	set output directory
version	set target TIA Portal version
{nouppgrade,cpuhmifirmwareonly, cpuhmifull, alldevicesfirmwareonly,alldevicesfull}	Chose between hardware upgrade strategy
Optional arguments	Description
-h, -help	show this help message and exit
-archive	set to save projects as archive files
-software	set to compile software
-hardware	set to compile hardware
-sivarc	set to generate HMI via SiVArc
-webblock	set to generate Webblock `

3.4 Operation python

“upgrader.py” skript can be executed directly with available python environment. The usage is the same as by the CLI. Python version 3.7.8 is recommended to use.

```
python upgrader.py [-h] [--archive] [--software] [--hardware] [--sivarc]
                  [--webblock]
                  inputpath outputpath version
{noupgrade,cpuhmifirmwareonly,cpuhmifull,alldevicesfirmwareonly,alldevicesfull}
```

3.5 Error handling

There is also a log file named “TiaScriptingModule.log” show the detail information of the upgrade status, including the error messages from TIA Scripting Module. You can check the issue if a project upgrade failed or upgraded with issues. The log file is placed in ErrorLog folder. “TiaScriptingModule.log” is created by TIA Scripting Module, so if environment variable is set, ErrorLog folder can be found there.

3.6 Known problems

- Upgrade of the projects where PLC-Webserver was enabled with version under TIA Portal 17, upgrade process might cause compile error.
Webserver certificate needed for S7-1500 firmware > V1.8 might cause a compile error.
Security mechanisms implemented in S7-1500 firmware > V2.8 might cause a compile error.
- Hardware Upgrade with option All devices might fail, because some devices are not changeable.
- The TIA Portal Project Upgrader is not capable of automatically installing the GSD(ML) files. Please Open project ones with UI and let install GSD(ML) files, before upgrading the project.

4 Appendix

4.1 Service and support

SiePortal

The integrated platform for product selection, purchasing and support - and connection of Industry Mall and Online support. The SiePortal home page replaces the previous home pages of the Industry Mall and the Online Support Portal (SIOS) and combines them.

- **Products & Services**
In Products & Services, you can find all our offerings as previously available in Mall Catalog.
- **Support**
In Support, you can find all information helpful for resolving technical issues with our products.
- **mySieportal**
mySiePortal collects all your personal data and processes, from your account to current orders, service requests and more. You can only see the full range of functions here after you have logged in.

You can access SiePortal via this address: sieportal.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page: siemens.com/sitrain

Industry Online Support app

You will receive optimum support wherever you are with the “Siemens Industry Online Support” app. The app is available for iOS and Android:



4.2 Links and literature

Table 3-1

No.	Topic
\1	SiePortal https://sieportal.siemens.com/
\2	Link to the entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109811744

4.3 Change documentation

Table 3-2

Version	Date	Modifications
V1.0.0	12/2021	Initial release with core functionality and UI adjustments
V1.0.1	12/2021	Minor cleanup, character encoding adjustments, and file management updates
V1.0.2	03/2022	Initial documentation, code cleanup, and bug fixes
V1.1.0	05/2022	FoSignificant development merge, build process improvements, and minor fixes
V2.0.0	07/2023	Major feature addition with TIA Scripting Module Project Upgrader and documentation updates
V2.0.1	10/2023	UI/UX improvements, hardware upgrade options, and bug fixes
V2.0.2	01/2024	Enhanced project recognition (zip files), storage handling, and documentation updates
V2.0.3	03/2024	New features including TIA scripting info, safety print handling, zip file scanning, and UI style improvements
V2.0.4	05/2024	Bug fixes for UI fields and crashes, automated build process, and documentation on known issues
V2.0.5	09/2024	CI/CD enhancements, TIA Scripting dependency updates, and comprehensive documentation releases
V2.0.6	12/2025	TIA Openness V21 support